VŠB – Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra informatiky

Možnosti poštovních serverů na Windows platformě

Mail Servers and their Possibilities on the Windows Platform

2010 Lenka Kučerová

Prohlašuji, že jsem tuto bakalářskou práci vypracovala samostatně. Uvedla jsem všechny literární prameny a publikace, ze kterých jsem čerpala.

V Ostravě 7. dubna 2010 .....

Předně bych ráda poděkovala vedoucímu bakalářské práce panu Ing. Lumírovi Návratovi, za pomoc při sestavení náplně bakalářské práce, za odborné vedení směřující ke splnění stanovených cílů a ochotu zodpovídat dotazy související s jejím zdárným vyhotovením.

Dále bych chtěla vyjádřit obrovské poděkování svým dětem, kterým jsem věnovala jen omezené množství volného času a v neposlední řadě poděkování náleží také manželovi, rodině a přátelům, za duševní podporu a trpělivost po celou dobu mého studia.

Abstrakt

Bakalářská práce popisuje možnosti poštovních serverů na platformě Windows, obsahuje popis instalace Exchange serveru 2007 ve firmách různých velikostí a uvádí vzorové příklady pro konfiguraci a správu tohoto poštovního systému.

V práci jsou popsány a porovnány poštovní servery Kerio Mail Server, IBM Lotus Domino a Microsoft Exchange Server. Následně je popsán návrh implementace Exchange Serveru 2007 do vytvořených modelů společností. Společnosti se liší jak počtem uživatelů poštovního systému, tak topologickým uspořádáním. Jednotlivé návrhy jsou dále doplněny o názorné tutoriály popisující průběh instalace. Poslední část je věnována správě a konfiguraci poštovního serveru Microsoft Exchange 2007 s použitím grafického rozhraní i příkazového řádku, tedy pomocí příkazů Exchange Management Shellu.

Klíčová slova: poštovní servery, Kerio, Lotus, Exchange, instalace, konfigurace

Abstract

Bachelor thesis describes possibilities of mail servers on the Windows platform, including Exchange server 2007 installation in companies of various sizes. There are practical examples of Exchange server configuration and management.

Thesis includes description and comparison of Kerio Mail Server, IBM Lotus Domino and Microsoft Exchange Server, followed by implementation design of Exchange 2007 server into specific company models. These companies differs both in number of users and also topological settings. Each design contains a particular tutorial of whole installation process. The last part is dedicated to administration and configuration of the Microsoft Exchange 2007 mail server using command line based Exchange Management Shell and Exchange console graphical interface.

Keywords: mail servers, Kerio, Lotus, Exchange, installation, configuration

Seznam použitých zkratek a symbolů

AD	–	Active Directory
ADAM	–	Active Directory Application Mode
CAS	–	Client Access Server, serverová role MS Exchange Serveru
CCR	–	Cluster Continuous Replication
CMS	–	Clustered Mailbox Server
DC	–	Domain Controller
DHA	–	Directory Harvest Attack
EAS	–	Exchange ActiveSync
EMC	–	Exchange Management Console
EMS	–	Exchange Management Shell
GC	–	Global Catalog
Hub	–	Hub Transport, serverová role MS Exchange Serveru
HQ	–	Headquarters
LCR	–	Local Continuous Replication
MBX	–	Mailbox, serverová role MS Exchange Serveru
MIME	–	Multipurpose Internet Mail Extensions
NLB	–	Network Load Balancing
NRPC	–	Notes Remote Procedure Call
RBL	–	Real-time block list
RC	–	Regional Center
RDP	–	Remote Desktop Protocol
RFC	–	Requests For Comments
RPC	–	Remote Procedure Call
SpoF	–	Single Point of Failure
UGMC	–	Universal Group Membership Caching
VSS	–	Volume Shadow Copy Service

Obsah

Seznam tabulek

Seznam obrázků

1 Úvod

Elektronická pošta patří k nejpoužívanějším službám internetu. Na její spolehlivosti a včasnosti doručování závisí chod nejedné společnosti. V době zadání tématu pro bakalářskou práci, byl ve společnosti, kde pracuji, implementován poštovní systém MS Exchange 2003. Poštovní systém společnosti Microsoft není však jediný, který lze na platformě Windows provozovat. Cílem práce je seznámit se s možnostmi dalších poštovních serverů, porovnat jejich vlastnosti a popsat zcela nově koncepčně přepracovanou verzi MS Exchange 2007, včetně instalace a správy.

V první části se ohlédneme téměř o padesát let zpět k prvním signálům elektronické komunikace a postupně se přeneseme přes důležité okamžiky vývoje až k poštovním systémům současnosti. Zmíníme požadavky a standardní vlastnosti e-mailových systému dnešní doby.

Další oddíl je věnován možnostem poštovních serverů, které lze provozovat na platformě Windows. Zde máme k dispozici produkty IBM Lotus Domino, Kerio Mail Server a Microsoft Exchange Server. Produkty jsou popisovány podle předem připravené šablony pro jednotnost a snazší orientaci. Výsledné porovnání uvedených poštovních serverů je mimo textové formy doplněno také přehledovou tabulkou.

Významná část práce se zaměřuje výhradně na poštovní server MS Exchange 2007. Na vytvořených modelech společností jsou demonstrovány možné návrhy implementace poštovního serveru včetně okomentování postupu návrhu. Nejvhodnější z nich je vybrán a doplněn o instrukce vedoucí k instalaci poštovního systému.

Poslední pasáž zachycuje základní přehled nastavení Exchange Serveru 2007. Prvky konfigurace a správy jsou popsány v blocích podle serverových roli nejprve z pohledu serverového nastavení a dále z pohledu konfigurace společnosti jako celku.

V kapitolách souvisejících s instalací a správou poštovního systému MS Exchange 2007 uvádím odkazy na obrazovková okna, jejichž číslování odpovídá označení v přílohách v samostatném elektronickém dokumentu.

1.1 Historie

Vznik elektronické pošty spojujeme s šedesátými léty 20.století a jejím využívání pro potřeby komunikace uživatelů mainfraimových počítačů se sdílením času. Tento princip vycházel z připojení pomocí terminálů k centrálnímu mainframe počítači, kde speciálně vytvořené programy zajišťovaly současný přístup účastníků na společné zdroje.

Time-sharing (sdílení času) označuje provozní formu, která umožňuje současný přístup více uživatelů. Přitom je každý uživatel v kontaktu se zařízením tak, jakoby ho měl k dispozici výhradně jen on. Přednosti velkého systému se tak otevírají všem uživatelům a existuje možnost interaktivního přístupu k centrálním datovým a programovým zdrojům. [2]

Odtud pochází i myšlenka vytvoření mailboxu jako elektronického úložiště dokumentů a souborů, umístěného na hlavním počítači. E-mailové zprávy pak byly zasílány z mailboxu v rámci jednoho počítače a ukládány do souboru v adresáři uživatele. Tyto zprávy sloužily spíše jako vzkazníky a nebylo možné je přenášet mezi počítači.

V roce 1971 odeslal americký počítačový technik Ray Tomlinson úspěšně první e-mail z jednoho počítače v síti ARPANET na druhý. Jako první také pro e-mailovou komunikaci použil znak "@" k oddělení jména uživatele a jména počítače.

V této době pak vznikalo a také zanikalo mnoho více či méně úspěšných speciálních programů pro síťovou komunikaci. Na rozvoj elektronické pošty měla podstatný vliv počítačová síť ARPANET a rozvoj internetu. To vedlo k nutnosti řešit otázky sjednocení informací, které jsou potřebné pro správné směrování datových paketů. Tyto informace (místo, datum, příjemce) tvořily hlavičku e-mailových zpráv a mohly být čteny pomocí řídících počítačů IMP (Interface Message Processors), které vytvářely datová spojení mezi hlavními počítači v topologii sítě.

První komerční softwarový balíček pro electronic mailing vytvořila roku 1976 společnost Computer Corporation of America, jmenoval se COMET a stál 40 000 dolarů; o málo později následoval program MESSENGER firmy On-line Software International jen za 18 000 dolarů. [2]

Veškeré technologické otázky a specifikace související s koordinaci počítačového síťového provozu jsou od roku 1969 definovány v RFC dokumentech a byly uveřejněny v roce 1983. Tyto dokumenty zahrnují standardy internetové komunikace a tedy i standardy pro přenos elektronických zpráv a používaných protokolů.

První úspěšné komerční e-mailové spojení bylo vytvořeno v roce 1989 mezi CNRI (Corporation for the National Research Initiative) a univerzitou v Ohiu. V roce 1993 byly připojeny na internet první elektronické poštovní systémy přístupné běžným uživatelům.

1.2 Současnost

V současnosti bezpochyby patří e-mailová komunikace k běžným součástem každodenního života. Pro svou rychlost, hromadnost a jednoduchost se tak jedná o velmi významnou formu komunikace. Díky pokročilým technologiím a standardu MIME jsme v rámci e-mailové zprávy schopni mimo textové informace přenášet také přílohy se soubory různých datových typů.

Náročnost současného člověka roste a tak přichází požadavky na integraci nových funkcí jakými jsou kalendáře, plánovače, zápisníky, možnosti sdílení kontaktů a jiných zdrojů, možnost čtení e-mailů v režimu offline (bez aktivního připojení k poštovní schránce) stejně jako možnost připojení se přes webové rozhraní nebo za pomocí mobilního telefonu. Nepostradatelnou součástí zvláště pro firemní e-mailové systémy jsou nabízená řešení pro archivaci a bezpečnost, které jsou již v systémech implementované nebo je lze o tyto funkce rozšířit.

Archivaci lze provádět jak na straně uživatele tak na straně serveru. Uživatel si může sám zálohovat vlastní poštovní schránku pomocí dostupných funkcí použitého poštovního klienta. Na straně serveru se může jednat o replikační mechanismy, vlastní zálohovací řešení nebo využití zálohovacích systémů třetích stran.

Bezpečnost z pohledu e-mailových systémů zahrnuje antispamovou a antivirovou ochranu. Spam neboli nevyžádaná pošta představuje až devadesáti procentní podíl veškeré elektronické komunikace a její včasnou filtrací zamezíme neefektivnímu vytěžování poštovních serverů. Nastavením filtračních pravidel můžeme identifikovat spamy, např. na základě kontroly obsahu e-mailu, kontrolou adres odesilatele a příjemce nebo kontrolou časových razítek. K dalším způsobům ochrany poštovních systémů patří ochrana proti neoprávněnému získávání e-mailových adres (DHA), ochrana proti odchytávání hesel (anti-phishing), ochrana proti proniknutí do systému na základě podvržené IP adresy (anti-spoofing), kontrola zda e-mail nebyl zaslán z počítače evidovaného jako rozesilatel spamů (RBL).

Antivirová ochrana může být řešena přímou integrací konkrétního antivirového produktu nebo implementací antivirového programu pro poštovní servery od libovolného výrobce.

Ve snaze přiblížit možnosti poštovních serverů na platformě Windows, budou popsány produkty tři významných společností - IBM Lotus Domino, Kerio Mail Server a Microsoft Exchange Server.

1.3 Elektronická zpráva

E-mailovou zprávu tvoří dvě hlavní části, kterými jsou hlavička a tělo zprávy. Hlavička e-mailové zprávy obsahuje povinná pole, která musí vyplnit odesilatel nebo jsou vyplňována automaticky systémem a dále pak nepovinná pole, jenž mohou být v případě potřeby vyplněna odesilatelem. Některá pole jsou doplňována v průběhu putování e-mailu od odesilatele k příjemci. Standardem formátu e-mailových zpráv se detailně zabývá RFC 822, standardem MIME rozšiřující standardní formát e-mailových zpráv pak RFC 2045 - RFC 2049.

1.4 Komunikační protokoly

SMTP (Simple MailTransfer Protocol) - Jednoduchý protokol pro přenos elektronické pošty v síti TCP/IP. Užívá se pro přenos zpráv od klienta pošty směrem k serveru a mezi poštovními servery. Zprávy ze serveru poštovní klient získává pomocí protokolu POP3 nebo IMAP4. [1]
Původní norma RFC 821 z roku 1982, byla v roce 2001 nahrazena novější RFC 2821.

POP3 (Post Office Protocol version 3) - Síťový protokol, který umožňuje přístup ke schránce elektronické pošty umístěné na jiném počítači zvaném poštovní server. Pozdější verze nejsou kompatibilní s dřívějšími. POP3 Extended Service rozšiřuje protokol pro práci s poštovními schránkami pro elektronické konference. [1]
Internetový protokol POP3 byl standardizován v roce 1996 v normě RFC 1939.

IMAP (Internet Message Access Protocol) - Protokol umožňující klientovi přístup a manipulaci s elektronickou poštou na serveru. Klient může vzdáleně vytvářet, mazat a přejmenovávat poštovní schránky (mailbox), vyhledávat v nich, přidávat atributy apod. Nezahrnuje funkce pro odesílání, k tomu využívá protokol (vt. SMTP). [1]
Nyní se používá protokol IMAP4, který je od roku 2003 definován v normě RFC 3501.

Vyjma uvedených standardních protokolů disponují někteří klienti e-mailových systémů vlastním komerčním protokolem např. Lotus Notes (NRPC) nebo Microsoft Outlook (MAPI).

MAPI (Messaging Application Programming Interface) - Rozhraní aplikačních programů k ovládání zpráv a elektronické pošty. MAPI umožnilo využít přenosové schopnosti elektronické pošty i pro přenos datových objektů, s nimiž tyto aplikace pracují. Např. uživatel textového editoru může odeslat právě zpracovaný dokument elektronickou poštou jinému uživateli, přímo z prostředí aplikace, s níž pracuje. Základ MAPI tvoří 12 funkcí, např. MapiDeleteMail(), MapiReadMail(), MapiSendMail() apod. [1]

NRPC (Notes Remote Procedure Call) - Nativní protokol společnosti IBM pro komunikaci klienta Lotus Notes s poštovním serverem Domino nebo Domino serverů vzájemně. Protokol využívá technologii typu klient - server pro vzdálené volání procedur.

2 Poštovní servery na platformě Windows

2.1 Kerio Mail Server

2.1.1 Popis společnosti

Hlavní ústředí Kerio Technologies se nachází v San Jose v Kalifornii. Kerio Technologies věnuje veškeré své úsilí distribuci a podpoře produktů, které zajišťují a chrání komunikaci v dnešním globalizovaném světě. Již více než 10 let poskytují dva vlajkové produkty společnosti Kerio Technologies, Kerio MailServer a Kerio WinRoute Firewall, malým a středně velkým podnikům na celém světě ty nejlepší nástroje pro e-mailovou komunikaci a internetovou bezpečnost. [4]

Kerio Technologies je poměrně mladá společnost, která se svým zaměřením orientuje především na vývoj softwarových produktů v oblasti komunikace a síťové bezpečnosti pro malé a středně velké firmy. Snaží se poskytovat kvalitní a cenově dostupná řešení. Její produkty se vyznačují jednoduchou instalací, snadnou správou a nízkými hardwarovými nároky.

Kerio Mail Server byl představen v roce 2002 jako groupwarový ekvivalent Microsoft Exchange. Společnost Kerio nabízí v rámci svého produktu procesy zpracování zpráv, správu a sdílení kalendářů, kontaktů, poznámek, úkolů a veřejných složek.

2.1.2 Popis produktu

Kerio MailServer je komplexní produkt pro e-mailovou komunikaci a týmovou spolupráci pro malé a střední organizace. Kombinuje funkce e-mailového a groupwarového serveru s antivirovou kontrolou, účinnou antispamovou ochranou, archivací, automatickým zálohováním a disponuje snadno použitelným webovým rozhraním pro správu. Kerio MailServer je řešením číslo jedna pro multiplatformní prostředí. [4]

Název produktu: Kerio Mail Server
Popisovaná verze : 6.7.0
Společnost : Kerio Technologies Inc.
Určen pro: malé a středně velké společnosti

Minimální požadavky na server pro 20 uživatelů
HW: CPU 1GHz, 512 MB RAM
Kapacita disku: instalace 50 MB + 40 GB pro schránky uživatelů a zálohy
OS: Windows 2000/XP/Vista/7, Windows Server 2003/2008

Instalované serverové komponenty
Kerio MailServer Engine – jádro systému
Kerio MailServer Monitor – komponenta pro monitoring stavu Engine
Kerio Administration Console – slouží pro administraci, správu, konfiguraci serveru a

uživatelských účtů. Umožňuje lokální i vzdálenou správu.
Performance – aplikace pro sledování výkonu

Klientské komponenty
Společnost Kerio neposkytuje vlastního e-mailového klienta.

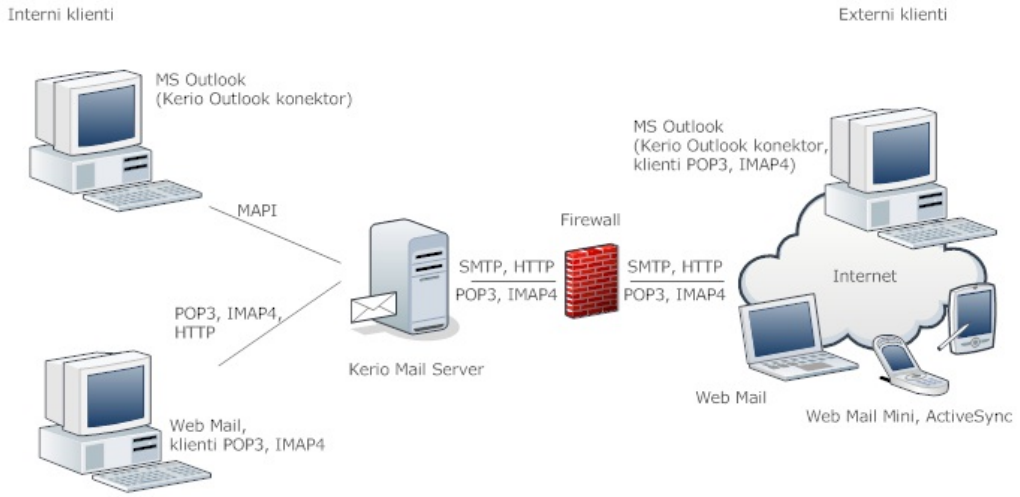
Konfigurační soubory
Konfigurační soubory mailserver.cfg pro serverové nastavení a users.cfg pro uživatele. Oba soubory obsahují konfigurační nastavení v XML struktuře. Jednotlivé parametry lze modifikovat v případě potřeby ručně či pomocí administrační konzole.

Uživatelské účty
Poštovní server umožňuje definovat uživatelské účty v rámci interní databáze manuálně, importem z externích zdrojů nebo namapováním pomocí adresářové služby Microsoft Active Directory. Dle způsobu definice uživatelských účtů využíváme pro správu interní databázi nebo adresářovou službu. Pro plnou integraci Microsoft Active Directory je nutné na server s adresářovou službou nainstalovat rozšíření Kerio Active Directory Extension, které umožní zobrazit a modifikovat nastavení vlastností spojených s poštovní schránkou pro jednotlivé uživatele, přímo v rámci Microsoft Active Directory. Kerio Active Directory Extension podporuje 64-bitové operační systémy.

Úložiště mailboxů
disk:\..\MailServer\store\mail\nazev_domeny\logon_name\
V tomto adresáři se nachází přesný obraz adresářové struktury jakou si uživatel vytvořil ve své poštovní schránce používáním libovolného klienta. V každém podadresáři je pak vytvořen adresář #msgs, kde se ukládají jednotlivé datové položky ve formě očíslovaných souborů typu .eml a soubor index.fld obsahující informace o každé zprávě v příslušném #msgs adresáři.

Klienti pro přístup k poštovní schránce
K připojení poštovní schránky lze použít libovolného poštovního klienta z libovolné platformy. Pro operační systém Windows se jedná o klienty Microsoft Outlook, Windows Mail a Windows Calendar. Připojení prostřednictvím webového rozhraní WebMail je podporováno internetovými prohlížeči Internet Explorer, Firefox a Safari. Připojení mobilním telefonem umožňuje pak webové rozhraní WebMailMini.

Bezdrátová synchronizace
Připojení a bezdrátová synchronizace je určena pro PDA a mobilní zařízení, která podporují ActiveSync. Pomocí funkce SmartWipe lze v případě ztráty mobilního telefonu vzdáleně vymazat veškerá jeho data. Funkce Smart Forward a Smart Reply umožňují minimalizovat objem přenesených dat souvisejících s načítáním příloh, určených pro další přeposlání. Podporován je Windows Mobile, Apple iPhone, Symbian, Palm a BlackBerry.



Obrázek 1: Kerio Mail Server - Infrastruktura

Zabezpečení
Poštovní server poskytuje antispamovou a antivirovou ochranu pro příchozí i odchozí zprávy. V rámci antispamu se jedná například o ochranu SpamAssassin pro kontrolu obsahu, ochranu proti neoprávněnému získávání e-mailových adres, odchytávání hesel, neoprávněnému proniknutí na základě podvržené IP adresy, kontrola zda e-mail nebyl zaslán rozesílatelem spamů.

V případě antivirové ochrany můžeme zakoupit licenci již s integrovaným McAfee antivirem nebo využít některý z integrovaných modulů pro práci s externími antivirovými programy, případně zkombinovat obě možnosti pro zesílení ochrany. Integrované moduly jsou určeny pro spolupráci s antiviry Avast, NOD32, AVG a Symantec.

Archivace a zálohování
Kerio Mail Server umožňuje provádět zálohování serverové konfigurace a poštovních schránek uživatelů. Zálohy lze plně automatizovat a v případě potřeby využít pro obnovení e-mailového systému na jiném serveru. Další možností je přeposílání kopií elektronických zpráv na vzdálený SMTP server. Pro archivaci dat je implementovaná služba, která vytváří komprimované soubory (zip) a ukládá je lokálně do speciálních archivních složek. Archivní složky jsou součásti poštovní schránky Administrátora.

2.1.3 Infrastruktura

Typické zapojení Mail Serveru Kerio je znázorněno na obr.1: Kerio Mail Server - Infrastruktura. Jedná se o samostatný poštovní server s interní databází uživatelských účtů, který podporuje přístup pomocí libovolných poštovních klientů včetně klientů určených pro mobilní zařízení, a přístup přes webové rozhraní.

2.1.4 Licencování

Kerio MailServer je zabezpečený poštovní server pro implementaci v malých a středně velkých společnostech. Základní licence je určena pro server a 10 uživatelů a cena se pohybuje kolem 12.850 Kč (bez DPH). Další rozšiřování licence se provádí dokupováním licencí po 5 uživatelích v ceně 504 Kč/uživatel (bez DPH). V ceně licence je zahrnuta aktualizace produktu a technická podpora po dobu 1 roku.

2.2 IBM Lotus Domino

2.2.1 Popis společnosti

IBM je americká společnost založena v roce 1911. Zabývá se prodejem a vývojem počítačů, softwaru, poskytováním služeb, poradenství a technických řešení na poli informačních technologií. Velkým přínosem pro rozvoj v softwarové oblasti bylo získání společnosti Tivoli System Corp. a Lotus Development Corp., kde v roce 1984 vzniká i Lotus Notes – komunikační aplikace založena na principu klient-server, která již v té době disponovala groupwarovými vlastnostmi. Později byl tento produkt přejmenován na Lotus Domino pro serverovou část a klientskou část Lotus Notes.

Dnes patří Lotus Domino k moderním serverům s groupwarovými vlastnostmi pro zpracování zpráv, dokumentů, diskusních fór a webových aplikací. Jedná se o aplikační databázový server s distribuovaným systémem. Aplikace běžící na Domino serveru jsou aktivními dokumentově orientovanými databázemi, kde základní jednotkou je dokument a každý dokument má své specifické vlastnosti. Jednotlivé dokumenty se prostřednictvím formulářů zobrazují v pohledech, které představují definovaný výběr dokumentů pomocí funkcí, příkazů, Java apletů či s využitím výkonných agentů.

2.2.2 Popis produktu

Softwarové produkty IBM Lotus Domino poskytují špičkové funkce pro podporu spolupráce, které lze implementovat jako hlavní infrastrukturu elektronické pošty a podnikového plánování nebo jako platformu obchodních aplikací, či případně v obou těchto rolích. Softwarový produkt Lotus Domino včetně svých softwarových klientů poskytuje spolehlivé a vícevrstvě zabezpečené prostředí pro rychlé předávání zpráv a spolupráci, jež podnikům pomáhá zvýšit produktivitu zúčastněných osob, optimalizovat obchodní procesy a posílit celkovou reakceschopnost. [5]

Název produktu: IBM Lotus Domino
Popisovaná verze : 8.5.1
Společnost : IBM
Určen pro: společnosti různých velikostí

Minimální požadavky na server pro 20 uživatelů
HW: Intel Pentium 1GHz, 512 MB RAM
Kapacita disku: 1,5 GB
OS:Windows Server 2003/2008

Instalované serverové komponenty
Domino Server – rozhraní, které zobrazuje hlášení o běžících serverových úlohách
Server Controler – prostřednictvím konzole řídí běh Domino serveru
Domino Console – rozhraní pro komunikaci se serverovým kontrolerem pomocí příkazů

Klientské komponenty
Lotus Notes – uživatelský klient, zahrnuje IBM Productivity Tools (obdoba MS Office)
Domino Administrator – administrační klient pro správu serveru, klientských účtů a databází
Domino Designer – pro přizpůsobení stávajících Lotus aplikací a tvorbu nových

Konfigurační soubory
Část konfigurace serveru je uložena v souboru notes.ini. Další konfigurační nastavení včetně struktury Domino Directory zahrnuje soubor names.nsf. Soubory typu *.ID jsou speciální klíče k serveru obsahující veškeré bezpečnostní údaje a informace o certifikačních autoritách.

K důležitým souborům souvisejícím s provozováním Domino Serveru patří soubory typu *.ntf představující šablony databází, log.nsf, který zaznamenává veškeré aktivity probíhající na serveru, mail.box představující úložiště právě odesílaných e-mailů a databáze administračního procesu admin4.nsf. Zde se shromažďují nastavené administrační procesy čekající na dobu, kdy mohou být spuštěny a bezchybně provedeny.

Uživatelské účty
IBM Domino server se vyznačuje vysokou mírou zabezpečení. Pro ukládání a udržování uživatelských účtů využívá vlastní adresářovou službu Domino Directory. Veškeré přístupy jsou řešeny pomocí certifikátů a ID souborů. ID soubor je speciálně vytvořený soubor pro každého uživatele, je generován při registraci uživatele do systému a obsahuje informace o certifikátech, digitálních podpisech, šifrovací a dešifrovací klíče a některé další údaje spojené s bezpečností. Využívá se zde RSA (RiverShamirAdleman) šifrování veřejným klíčem.

Úložiště mailboxů
disk:\.. \Lotus\Domino\Data\mail\logon_name.nsf
Pro každého uživatele poštovního systému je vytvořena vlastní databáze v souborovém systému serveru – jediný soubor, který obsahuje veškerá data spojená s poštovní schránkou uživatele, e-maily, kontakty, kalendářové položky, úkoly, poznámky a vlastní nastavení.

Klienti pro přístup k poštovní schránce
Společnost IBM poskytuje vlastního poštovního klienta Lotus Notes. Komunikace klienta a Domino serveru nebo Domino serverů vzájemně zprostředkovává nativní protokol NRPC. Server Lotus Domino podporuje přímé připojení klienta MS Outlook a připojení libovolných klientů pomocí IMAP nebo POP3. K podporovaným standardům patří přístup přes webové rozhraní.

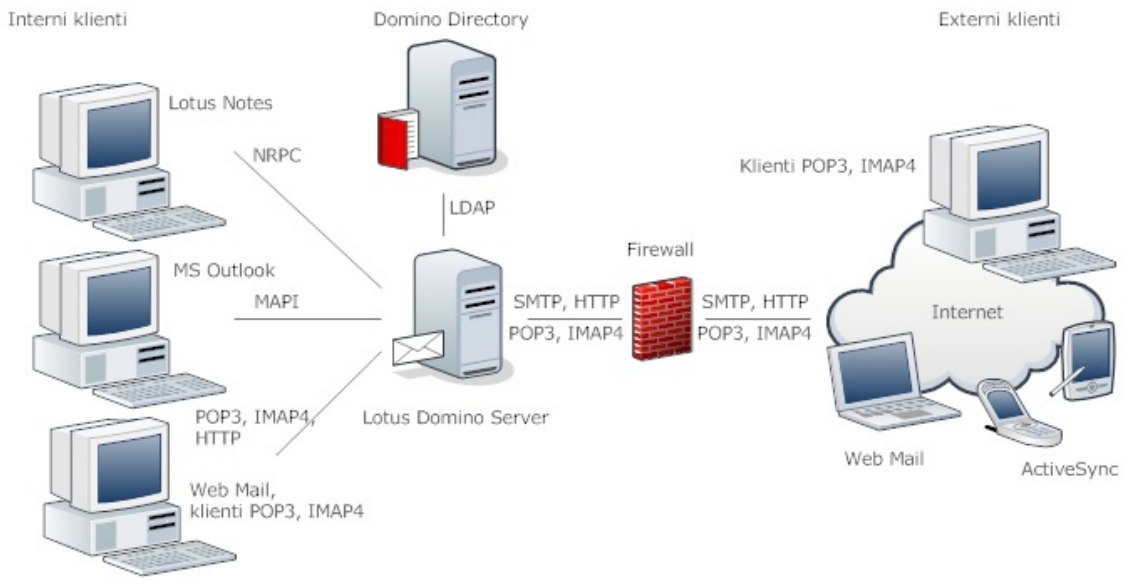
Bezdrátová synchronizace
IBM Lotus Notes Traveler poskytuje připojení a bezdrátovou synchronizaci poštovní schránky na přenosných zařízeních Microsoft Windows Mobile (smartphone nebo Pocket PC) a vybraných typech mobilních telefonů Nokia se systémem Symbian S60. Od verze Lotus Notes Travel 8.5.1 je podporována bezdrátová synchronizace pro iPhone prostřednictvím ActiveSync.

Zabezpečení
Poštovní server Lotus Domino zajišťuje výkonné antispamové funkce a umožňuje přizpůsobení filtrace požadavkům společnosti. Toto lze provést úpravou výchozích hodnot serverového nastavení pro SMTP komunikaci, vytvořením vlastních seznamů povolených a nepovolených odesilatelů. Antivirová ochrana není řešena, resp. máme možnost pořídit si produkt společnosti IBM Lotus Protector for Mail Security nebo využít některou z nabídek třetích stran.

Archivace a zálohování
Poštovní databáze mohou být umístěny na více serverech současně. Jejich synchronizace probíhá formou replikací. Takto udržované repliky mohou sloužit jako zálohy v případě poškození databáze. Pro rozsáhlejší poštovní systémy se pro zvýšení dostupnosti a rozložení zátěže implementují clusterové řešení. Další možností pro zálohování a případnou obnovu dat Lotus Domino serveru je využití produktu IBM Tivoli Storage Manager for Mail nebo zálohovací systémy jiných výrobců. Pro implementaci archivačních mechanismů využijeme nabízená řešení třetích stran.

2.2.3 Infrastruktura

Obr.2: IBM Lotus Domino - Infrastruktura zobrazuje jádro poštovní systému, které tvoří Lotus Domino Server a Domino Directory. Pro přístup k obsahu mailboxů umístěných na Lotus Domino Serveru je požadováno ověření uživatele pomocí Domino Directory. K elektronické poště přistupujeme klienty Lotus Notes, MS Outlook, libovolnými poštovními klienty, webovým rozhraním či mobilním zařízením.



Obrázek 2: IBM Lotus Domino - Infrastruktura

2.2.4 Licencování

Licencování se provádí dvojím způsobem. U rozsáhlých společností s více než 1000 uživateli se řídí způsobem klient – server. Tedy vedle pořízení Domino serveru, který je licencován podle počtu fyzických procesorů, je také nutné zakoupení klientských licencí pro každého uživatele.

Serverové licence:
Lotus Domino Messaging Serveru (29.268 Kč bez DPH/CPU) - poštovní server
Lotus Domino Enterprise Server (75.782 Kč bez DPH/CPU) - poštovní a aplikační server
Lotus Domino Utility Server Express (63.932 Kč bez DPH/CPU) – licence zahrnuje přístup ke všem typům aplikací Lotus Domina, ale neopravňuje k využívání služeb poštovního serveru. Je uveden pro úplnost licenčních možností.

U klientských licencí vybíráme dle potřeby z následujících produktů :
IBM Lotus Notes for Messaging (2.570 Kč bez DPH)
IBM Lotus iNotes (Domino Web Access) for Messaging (1.540 Kč bez DPH)
IBM Lotus Notes for Collaboration (3.580 Kč bez DPH)
IBM Lotus iNotes (Domino Web Access) for Collaboration (2.370 Kč bez DPH)
IBM Lotus Traveler – klient pro bezdrátovou synchronizaci pomocí rozhraní ActiveSync je volně dostupný pro majitele výše uvedených licencí (Notes nebo iNotes)

Další možností, výhodnou především pro malé a střední společnosti do 1000 zaměstnanců, je pořízení speciální Express edice (Lotus Domino Messaging Express a Lotus Domino Collaboration Express), kde není zapotřebí opatřit server samostatnou licencí, ale licencování se řídí pouze počtem uživatelů.

Lotus Domino Messaging Express – poštovní server pro malé a střední společnosti umožňující využívání víceúrovňového zabezpečeného e-mailu, kalendářů, plánování a diskusních fór týmových prostorů. Neopravňuje k využívání produktu IBM Lotus Sametime. Jeho cena se pohybuje kolem 2.700 Kč bez DPH.

Lotus Domino Collaboration Express – rozšiřuje produkt Lotus Domino Messaging Express o možnost spouštění vlastních aplikací a aplikací nezávislých dodavatelů postavených na softwaru Lotus Domina. Cena licence je 3.780 Kč bez DPH/uživatel.

Veškeré licence jsou platné 1 rok a po dobu platnosti zahrnují technickou podporu.

Nutno zmínit, že společnost IBM vychází vstříc svým zákazníkům a v rámci zakoupení licencí podporuje omezené využívání některých svých dalších produktů. U serverového licenčního oprávnění se jedná o produkty Tivoli Directory Integrator, DB2 Enterprise a WebSphere Application. Z pohledu licencí klientů je k dispozici např. IBM Lotus Symphony.

2.3 MS Exchange Server

2.3.1 Popis společnosti

Společnost Microsoft byla založena v roce 1975 a je světovým lídrem v poskytování softwaru, služeb a řešení, které pomáhají lidem a firmám po celém světě plně realizovat jejich potenciál. Česká pobočka společnosti Microsoft Corporation zahájila svoji činnost v roce 1992. Od října roku 2007 ji vede Jane Gilson. [6]

Americká společnost Microsoft se od svého vzniku věnovala vývoji softwaru. Vedle programovacích jazyků, operačních systémů a kancelářských aplikací se zabývá vývojem produktů určených pro podnikové informační systémy. Do této kategorie patří Exchange Server, SharePoint Server, Office Communicators Server, ISA Server a Forefront. Z oblasti hardwaru se jedná především o výrobky zajišťující pohodlí uživatele (myš, joystick, herní konzole, ergonomická klávesnice, wi-fi router, web kamera).

Vývojem Exchange Serveru se společnost Microsoft zabývá od roku 1993. V současné době poštovní server nabízí kromě množství funkcí pro komunikaci a týmovou spolupráci, také moderní technologie přístupu, zabezpečení vysoké dostupnosti a nástroje pro kontrolu konfigurace poštovního systému.

2.3.2 Popis produktu

Díky nejnovější verzi systému Exchange může firma dosáhnout lepších výsledků a zároveň mít pod kontrolou náklady na nasazení, správu a dodržování předpisů. Systém Exchange nabízí nejširší paletu možností nasazení, integrované funkce ochrany před únikem informací a pokročilé funkce pro zajištění dodržování předpisů, které dohromady tvoří nejlepší řešení pro zasílání zpráv a spolupráci dostupné na trhu. [6]

Název produktu: Microsoft Exchange Server 2007
Popisovaná verze : 08.02.0176.002
Společnost : Microsoft
Určen pro: společnosti různých velikostí

Minimální požadavky na server pro 20 uživatelů
HW: počítač s architekturou x64 a 64 bitovým procesorem, 2 GB RAM
Kapacita disku: 1,2 GB pro instalaci na jednotce, kde bude Exchange Server 2007 instalován + 200 MB na systémové jednotce
OS:Windows Server 2003/2008 v 64 bitové verzi

Instalované serverové komponenty
Client Access Server - role pro přístup k poštovním schránkám pomocí libovolných klientů s výjimkou přímého přístupu MAPI klienta Outlook
Hub Transport – role pro zpracování a směrování pošty v rámci exchange organizace, doručuje e-maily do poštovních schránek příjemců umístěných na mailbox serveru a také adresátům v síti Internet
Mailbox – role zahrnující databáze poštovních schránek a veřejných složek
Unified Messaging – role integrující možnosti hlasové pošty, faxových a e-mailových služeb do jedné unifikované schránky, propojuje Exchange Server 2007 s existující telefonní síti společnosti
Edge Transport – role s funkcí antispamové ochrany, umožňuje filtrování zpráv, nastavení pravidel přenosu, nastavení doménové bezpečnosti, tato serverová role se instaluje na samostatně stojící server na hranici topologie, v tzv. perimetru nebo demilitarizované zóně

Exchange Management Shell – administrátorská konzole pro administraci pomocí příkazů Windows PowerShellu. Umožňuje provádění administračních úkonů opakovaně pomocí scriptů
Exchange Management Console – administrátorská konzole s grafickým uživatelským rozhraním založená na technologii Windows PowerShell. Veškeré administrátorské příkazy jsou zároveň zobrazovány v příkazových formulích (cmdlets)

V rámci EMC jsou poskytovány nástroje pro diagnostiku a odstraňování potíží :
Exchange Best Practices Analyzer – nástroj pro kontrolu konfigurace exchange serverů, na případné chyby upozorní a navrhne řešení

Exchange Mail Flow Troubleshooter – nástroj pro diagnostiku odstraňování potíží s tokem zpráv
Exchange Databáze Troubleshooter – nástroj pro odstraňování potíží s připojením databází a správou skupinových úložišť pro obnovení databází
Exchange Performance Troubleshooter – nástroj pro odstraňování potíží s výkonem aplikace Outlook a Exchange serveru

Klientské komponenty
MS Outlook 2007 – uživatelský klient pro zprávu elektronické pošty a spolupráci, je součástí kancelářského balíku Microsoft Office 2007.

Konfigurace systému
Exchange Server společnosti Microsoft je plně integrován s operačním systémem Windows Server a s adresářovou strukturou Active Directory, kde je také uložena jeho konfigurace.

Uživatelské účty
Uživatelské účty jsou uloženy v centrální databázi adresářové služby Active Directory. K získávání těchto údajů se využívá LDAP. Pokud se uživatel přihlásí do domény, je ověřen pomocí Active Directory a jeho autentizační údaje jsou předány na Exchange server. To znamená, že pro přístup k poštovní schránce není další ověřování požadováno. Správa přímo související s příjemci elektronické pošty resp. s využíváním poštovních schránek je oddělena od správy objektů Active Directory. Provádí se z Exchange Management Console nebo pomocí příkazů PowerShellu z administrační konzole Exchange Management Shell.

Úložiště mailboxů
disk:\..\StorageGroup\MailBoxDatabase.edb
Na serveru s instalovanou serverovou rolí Mailbox, jsou uloženy databáze poštovních schránek a veřejných složek. Databáze jsou seskupovány do skupinových úložišť (Storage Groups). V jednom úložišti může být až pět databází. Každé úložiště je spravováno samostatným serverovým procesem. S ohledem na zálohování a případnou obnovu, se však doporučuje umisťovat pouze jednu databázi do jednoho úložiště.

Klienti pro přístup k poštovní schránce
Poštovní klient Outlook 2007 se připojuje přímo k mailbox serveru pomocí protokolu MAPI. Připojení ostatními typy klientů je zajišťováno serverovou rolí Client Access Server. K poštovní schránce můžeme přistupovat libovolným klientem podporující protokol POP3 nebo IMAP4, přes webové rozhraní Outlook Web Access z libovolného webového prohlížeče, nebo pomocí Outlook AnyWhere. Outlook AnyWhere je nové pojmenování pro komunikaci Outlooku a Exchange serveru přes internet. Tato technologie umožňuje zabalit komunikaci RPC do protokolu HTTPS.

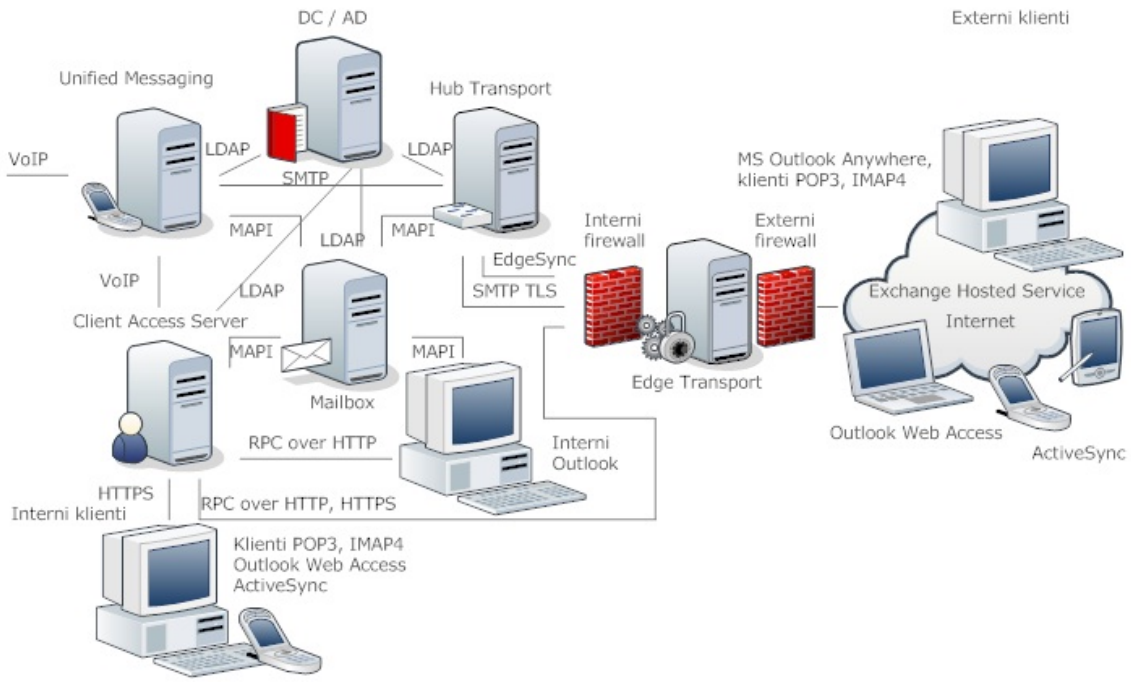
Bezdrátová synchronizace
Microsoft Exchange Server 2007 podporuje oboustrannou synchronizaci obsahu poštovní schránky s mobilními zařízeními, které podporují ActiveSync. Mezi tyto zařízení patří PDA, Smartphone a vybrané typy mobilních telefonů Nokia, Sony-Ericsson, Palm a některá další. Exchange ActiveSync umožňuje také nastavení bezpečnostních politik pro zablokování přístroje či smazání všech dat.

Zabezpečení
Poštovní server nabízí velmi účinnou antispamovou ochranou v rámci serverové role Edge Transport. Pokud tato role není implementována, lze antispamovou ochranu přenést na serverovou roli Hub Transport. Antispamová ochrana zajišťuje filtrování připojení na základě seznamů povolených a blokovaných IP adres, včetně kontroly RBL. Dále filtrování podle důvěryhodnosti adres odesílatelů a příjemců a také dle hodnocení obsahu zpráv.

Antivirová ochrana je nabízena v rámci produktu Forefront Security pro Exchange server. Lze jej instalovat s rolemi Mailbox, Edge Transport a Hub Transport. Forefront umožňuje integraci až pěti z devíti nezávislých skenovacích modulů různých společností. Tyto moduly provádějí antivirovou kontrolu a umožňují filtraci příloh podle velikosti, obsahu nebo typu souboru a to včetně komprimovaných souborů.

Dalším možným způsobem zabezpečení je využití hostovaného filtrování Exchange Hosted Service. Tato služba je provozována v globální síti datových center společnosti Microsoft, které přijímají e-mailovou komunikaci jménem zákazníků. Exchange Hosted Service provádí antivirovou kontrolu, filtraci nevyžádané pošty a pouze čisté e-mailové zprávy přeposílá zabezpečeným protokolem SMTPs do sítě zákazníka.

Archivace a zálohování
K zálohování dat lze využít Streaming backup a Volume Shadow Copy Service. Tyto technologie jsou určeny pro zálohy Microsoft Windows Serveru a podporují záloho- vání dat Microsoft Exchange Serveru. Pro účely archivace můžeme využít software třetích stran, např. EMC MailXtender. Určitou úroveň ochrany dat poskytují mechanizmy využívané pro zvýšení dostupnosti - replikace. K dispozici máme Local Continuous Replication v rámci jednoho serveru nebo Cluster Continuous Replication, kdy se vytváří kopie celého uzlu v clusteru. Replikace zajišťuje kopírování transakčních logů z aktivní databáze do pasivní kopie. Ačkoliv replikace neslouží jako náhrada zálohování, umožňuje snížit frekvenci provádění pravidelného zálohování dat Exchange Serveru.



Obrázek 3: MS Exchange Server - Infrastruktura

2.3.3 Infrastruktura

Infrastruktura poštovního systému MS Exchange Server 2007 zahrnuje serverové role Mailbox, Hub Transport, Client Access Server a Unified Messaging v interní AD struktuře a Edge Transport na hranici topologie (Obr.3: MS Exchange Server - Infrastruktura). Ověřování uživatelů probíhá pomocí Active Directory. Server podporuje používání libovolných poštovních klientů, přístup přes webové rozhraní, hlas nebo mobilní zařízení. Nativním klientem je MS Outlook.

2.3.4 Licencování

Exchange Server 2007 je vydán ve dvou edicích. Standard Edition pro malé a střední společnosti, Enterprise Edition pro velké korporace.

Serverová licence:
Standard Edition - nabízí připojení maximálně pěti neomezeně velkých databází. Základní cena Exchange Server 2007 + 5x Standard CAL pro klienty činí 40.390 Kč (bez DPH).
Enterprise Edition - umožňuje vytvoření až padesáti databází, podporuje clusterové technologie Single Copy Cluster a Cluster Contionuous Replication. Cena 218.450 Kč (bez DPH) zahrnuje Exchange Server 2007 Enterprise Edition a 25 klientských licencí Standard CAL.

Klientské licence:
Standard CAL – základní klientská licence udělující právo přístupu k službám Exchange Serveru pro oba typy serverových edicí (Standard i Enterprise). Zahrnuje plný klientský přístup, využívání sdílených kalendářů, přístup mobilních zařízení a antispamovou ochranu. Její cena se pohybuje kolem 2.180 Kč (bez DPH)
Enterprise CAL – rozšíření licence Standard CAL stojí 1.120 Kč (bez DPH) a opravňuje k využívání následujících služeb:
Unified Messaging - pro propojení služeb poštovního serveru s hlasovými službami
Journaling – pro sledování aktivit uživatelů
Spravované složky – zahrnuje další složky v mailboxech uživatelů, které podléhají plné definici a správě administrátorům Exchange serveru

Enterprise CAL +Software Assurance
Hostované filtrování – využívání „předsunutého“ serveru za účelem filtrace nežádoucích zpráv
Forefront Security pro Exchange – zahrnuje antivirovou a antispamovou ochranu

Klientské licence lze pořídit také jako součást klientského balíčku:
Core CAL obsahuje licenci Exchange Standard CAL
Enterprise CAL Suite zahrnuje obě licence Standard CAL i Enterprise CAL

Přístupové klientské licence nezahrnují licenci na Outlook 2007, který je součástí balíku Microsoft Office 2007 a řídí se samostatným licencováním.

2.4 Porovnání poštovních serverů

Otázkami, které jsou spojené s porovnáváním poštovních serverů, se zabýváme především v souvislosti s pořízením vlastního elektronického poštovního systému. Při výběru, ať už se jedná o první implementaci či nutnost zmodernizovat stávající, nevyhovující systém, je potřeba vždy zohlednit potřeby a požadavky dané společnosti. Z tohoto hlediska posuzujeme velikost společnosti co do počtu uživatelů, počtu připojených poboček, možnost přístupu k obsahu poštovních schránek, náročnost z pohledu administrace a v neposlední řadě cenu související s pořízením a údržbou systému.

Poštovní server Kerio patří k menším poštovním systémům. Je vhodný pro malé a střední společnosti. Většina zákazníků společnosti Kerio pokrývá potřeby do 500 uživatelů soustředěných do jednoho místa, případně rozmístěných do hlavního firemního sídla a jedné pobočky. Instalaci lze provést na běžný osobní počítač, který nemusí být členem domény a využívat adresářovou službu Active Directory. Z toho pramení nízké pořizovací náklady na HW i operační systém počítače.

Ceny licencí poštovního serveru jsou jistě také velmi zajímavé pro menší typy společností a způsob licencování je ve srovnání s rozsáhlejšími produkty mnohem transparentnější. Nákup se řídí pouze počtem uživatelů, aniž bychom museli rozlišovat způsoby jakými se

klienti budou ke svým poštovním schránkám připojovat. Pokud bude využíváno pouze webového rozhraní a možnosti synchronizace dat s mobilními přístroji, nejsou další poplatky nutné.

Společnost Kerio nemá vlastního poštovního klienta, jedná se zde pouze o serverovou část poštovního systému. Budeme-li chtít využívat služeb klienta, máme možnost využít MS Outlook, který je součástí produktu MS Office a vztahují se na něj licenční předpisy společnosti Microsoft. Podporováni jsou také poštovní klienti založeni na standardních komunikačních protokolech POP3 nebo IMAP4.

Pokud pomineme klientskou část systému a vrátíme se k serverové nelze přehlédnout možnost integrované antivirové ochrany a schopnost archivace dat. Data jsou ukládána jako samostatné soubory v souborovém systému, nevyužívá se databázových úložišť. Archivace dat spočívá v komprimaci souboru do formátu zip, obnova je skutečně snadná. Náročná není ani administrace systému. Pomocí jednoduchého uživatelského rozhraní lze nastavit vše potřebné a vlastně se toho nedá ani moc pokazit. Kerio MailServer je funkční systém.

IBM Lotus Domino je systém určen pro společnosti různých velikostí. Systém zde představuje server, u kterého máme v závislosti na typu licence možnost volby využití. K výběru se nabízí poštovní server, aplikační server nebo kombinace uvedených možností. Aplikační server opravňuje ke spouštění a používání aplikací postavených na softwaru Lotus Domino. To znamená, že pokud takový software již využíváme nebo plánujeme využívat, budeme muset vlastnit příslušný typ licencí pro server i klienty. Navíc pořízením licence Domino Designer (20.700 Kč bez DPH) získáme oprávnění i prostředí k tvorbě vlastních aplikací.

IBM Lotus Notes je klient Domino serveru. Slouží jako klient elektronické pošty i klient aplikací a v obou případech podporuje používání kancelářských nástrojů. To znamená, že budeme mít k dispozici sadu aplikací, které svou povahou odpovídají balíku MS Office.

Výhodou kombinace aplikačního a poštovního serveru je pak používání jednotného prostředí se shodnými nebo velmi podobnými vlastnostmi (ovládací prvky, design, menu, funkce spojené s využíváním dokumentově orientovaných databází).

Licenční systém rozděluje zákazníky dle počtu uživatelů do dvou skupin. Pro první skupinu, společnosti do 1000 uživatelů, je připraven zvýhodněný systém licencování, který se řídí pouze poč- tem uživatelů. Druhá skupina zahrnuje společnosti s počtem uživatelů nad 1000, kdy mimo počtu uživatelů a zvolených typů klientů je nutné opatřit licencí také server. Licencování serveru se vztahuje k počtu procesorů. Právě z důvodu licencování dle procesorů a odhadům zamýšleného připojení uživatelů se tato licenční politika, z mého pohledu, řadí ke složitějším.

Za složitější považuji také administraci systému. Pro správu slouží serverové dokumenty a konfigurační dokumenty. V každém typu dokumentů jsou možnosti nastavení rozprostřeny do víceúrovňových menu a ne vždy se zobrazované nastavení vejde na jednu obrazovku. Navíc některá nastavení, pro dosažení požadované funkčnosti, jsou nutná provést na dvou místech.

Na druhou stranu množství nastavení nám umožňuje maximálně přizpůsobit funkčnost serveru potřebám společnosti. Systém správy i s použitím grafické administrační konzole je poněkud nepřehledný, vyžaduje odborné znalosti a tudíž je nutné mít k dispozici schopného administrátora, ostatně jako u většiny rozsáhlejších systémů. Domino server se instaluje na server s operačním systémem Windows 2003 nebo Windows 2008 a s odpovídajícím HW vybavením.

Veký důraz je kladen na zabezpečení přístupu. K ověřování se využívá certifikátů a adresářové služby Domino Directory. Samotný poštovní server resp. Domino server používaný pouze pro zpracování elektronické komunikace využívá ukládání dat do domino databází samostatně pro každého uživatele. Umožňuje vytvořit rozsáhlou firemní infrastrukturu propojením libovolného počtu poboček a vytvořením příslušných connection dokumentů.

Repliky databází můžeme vytvářet lokálně i mezi vzdálenými servery. Pro rozsáhlé systémy lze využít možnosti clusteringu na aplikační úrovni, tzn. že instalace není podmíněna shodným HW, OS ani verzí Domina. Zvážením veškerých potřeb společnosti můžeme pomocí Lotus Domino serveru vytvořit výkonný informační systém pokrývající aplikační i poštovní potřeby společnosti.

Microsoft Exchange server je samostatný produkt zabývající se pouze zpracováním elektronické komunikace a v rámci licence nezahrnuje rozšíření podobná aplikačnímu serveru společnosti Lotus. Od verze 2007 plně využívá 64-bitové architektury. K dispozici je i 32-bitové vydání určené pouze k testovacím účelům.

Poštovní systém Exchange je založen na serverových rolích. Serverových rolí je pět (Client Access Server, Hub Transport, Mailbox, Unified Messaging a Edge Transport) a určují jakou funkci bude server v rámci poštovního systému zastávat. Neznamená to však, že k nasazení systému je zapotřebí pěti fyzických strojů. Systém se instaluje na servery s 64 bitovým operačním systémem Windows Server 2003 nebo 2008 a mimo role Edge Transport lze všechny ostatní instalovat na jeden fyzický server.

Členění systému na role přináší možnost instalovat na každý server jen potřebné komponenty k plnění určité funkčnosti. Využití je zřejmé zejména u rozsáhlejších poštovních systémů, kde je nutné zapojení více serverů. Pak nemusíme na každý server instalovat celou poštovní aplikaci, ale pouze určitou serverovou roli.

Exchange server je integrován s operačním systémem Windows. Pro ověřování uživatelů využívá adresářovou službu Active Directory.

Způsob licencování odpovídá přidělování oprávnění produktům společnosti Microsoft a jeví se být transparentnější než u Lotus Domina. Serverové edice jsou dvě, základní pro připojení pěti databází a rozšířená zahrnuje padesát připojených databází a funkce clusteringu. Databáze představuje úložiště libovolného počtu poštovních a zdrojových schránek a její velikost není omezena resp. je omezená pouze kapacitou diskového pole.

Klientské licence jsou také dvě a liší se především možností využívání služeb Unified Messagingu a právě možnost hlasového přístupu k datům poštovní schránky neumožňuje v současné době žádný jiný z uvedených poštovních serverů. Součástí klientského opráv- nění není licence na MS Outlook.

Pro správu systému je připraveno vcelku přehledné a intuitivní grafické uživatelské rozhraní bez víceúrovňových systémů menu a administrátorská konzole pro správu pomocí příkazů. Administrace Exchange serveru je založena na Windows PowerShellu a vyžaduje alespoň základní znalosti řádkových příkazů. Výhodou je jistě schopnost tvorby scriptů pro usnadnění a zautomatizování některých úkonů správy.

Poštovní systém také podporuje replikační mechanismy u obou typů serverových licenčních oprávnění a umožňuje rozšíření o implementaci antivirové ochrany. MS Exchange 2007 poskytuje velice propracované koncepční řešení poštovního systému. Vyvinutý systém serverových rolí, správy a možnosti přístupových technologií řadí MS Exchange 2007 k moderním a výkonným poštovním serverům, který je schopen uspokojit potřeby i skutečně velkých korporátních organizací.

Pozn.: Uvedené ceny jsou pouze orientační a jsou čerpány z dostupných ceníků (říjen 2009) českých případně zahraničních obchodních partnerů posuzovaných společností.

Poštovní server	Kerio Mail Server 7.6.0	IBM Lotus Domino 8.5.1	Microsoft Exchange 2007
implementace dle velikosti firem	malé a střední	bez omezení	bez omezení
OS poštovního serveru	Windows 2000/XP Windows Vista/7 Windows Server 2003/2008	Windows Server 2003/2008	64-bitové verze Windows Server 2003/2008
ověřování a správa uživ. účtů	vlastní, možnost mapování z AD	Domino Directory	Active Directory
antispamové funkce	ano	ano	ano
antivirové zabezpečení	ano, v rámci rozšiřující licence	ne, možnost dokoupení : Lotus Protector for Mail Security	ano, možnost rozšíření o Forefront Security nebo sjednání služby Exchange Hosted Service
archivace, zálohy	ano, ano	ne, formou replikací	ne, streaming backup,VSS
podpora práce v clusteru	ne	ano, aplikační úroveň	ano, OS Level
nativní klient	ne	Lotus Notes	MS Outlook
ostatní podporovaní klienti	libovolný klient POP3, IMAP MS Outlook	libovolný klient POP3, IMAP MS Outlook	libovolný klient POP3, IMAP
přístup přes webové rozhraní	ano	ano	ano
hlasový přístup (VoIP)	ne	ne	ano
synchronizace dat s mobilními přístroji	ano	ano	ano
diskusní fóra	ne	ano	ne
zkušební verze	30 denní	90 denní	120 denní
pořizovací HW náklady	nízké	střední	vysoké
náklady na pořízení licencí	nízké	střední - vyšší	vysoké

Tabulka 1: Porovnání poštovních serverů

3 Instalace Exchange Serveru 2007

V této části se budu zabývat výhradně produktem pro zpracování elektronické komunikace společnosti Microsoft. Vytvořím modelové příklady společnosti různých velikostí a popíši jejich požadavky na vytvářený e-mailový systém. S ohledem na definované požadavky navrhnu implementaci nového poštovního systému Microsoft Exchange Serveru 2007 pro každý typ společnosti. Následně jednotlivé implementace doplním tutoriály popisující průběh instalací.

Jednotlivá řešení se budou vztahovat k instalacím Exchange Serveru do již připraveného firemního prostředí - počítačové sítě s adresářovou službou Active Directory. Technické požadavky související s přípravou fyzických serverů k implementaci poštovního systému jsou společné, proto budou uvedeny v příloze.

3.1 Malá společnost

3.1.1 Model

Popis

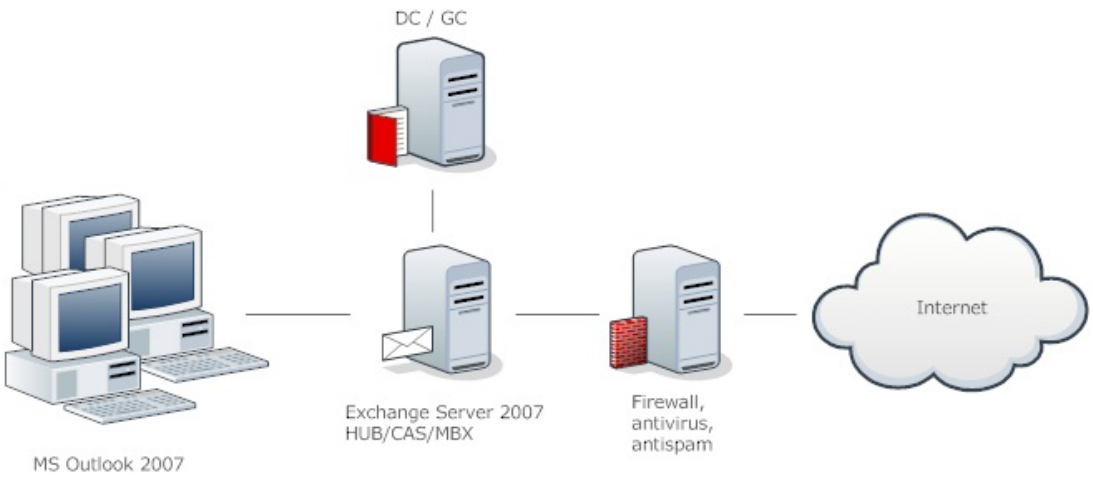
Malá společnost, se sídlem v Brně, se zabývá opravami elektrospotřebičů. Ve společnosti je 50 zaměstnanců – uživatelů elektronického poštovního systému. E-mailová komunikace je využívána ke komunikaci se zákazníky a s dodavateli náhradních dílů pouze v pracovní době (pracovní dny 8:00-18:00).

Jedná se o společnost soustředěnou do jednoho místa, bez dalších poboček.

Společnost se rozhodla přejít od hostovaného řešení k implementaci vlastního e-mailového systému. Data ze stávajícího systému budou převáděna pomocí importů PST souborů v aplikaci MS Outlook 2007. E-mailové zprávy jsou dosud stahovány z hostitelského systému pomocí protokolu POP3.

Současný stav sítě

- Společnost má samostatnou Active Directory doménu
- V doméně je instalován Domain Controller, který je konfigurován jako GC
- Společnost je připojena k Internetu přes firewall
- Administrace systému je prováděna externím pracovníkem



Obrázek 4: Malá společnost - Návrh Infrastruktury

Požadavky

- přístup k mailboxům je požadován pouze z vnitřní sítě
- uživatelé se budou připojovat k mailboxům pomocí klienta MS Outlook 2007

3.1.2 Návrh infrastruktury

Před samotnou instalací Exchange Serveru 2007 je potřeba navrhnout infrastrukturu dle konkrétních potřeb společnosti. Pro 50 zaměstnanců pracujících v jednom místě využijeme možnost instalace rolí Mailbox, Client Access Server a Hub Transport na jeden fyzický server (Obr.4 : Malá společnost - Návrh Infrastruktury).

Antivirovou ochranu a filtrování spamu bude zajišťovat aplikační firewall společnosti. Na firewallu poběží SMTP server, který poštu přijme, oskenuje a odešle na Exchange Server. Na firewall budou nastaveny MX záznamy pro směrování pošty z internetu. Odchozí elektronická komunikace bude rovněž směrována přes podnikový firewall do internetu.

3.1.3 Instalace Exchange Serveru 2007

Vybraný fyzický server připravíme dle přílohy Příprava k instalaci Exchange Serveru 2007. Pro implementaci poštovního systému zvolíme Exchange Server 2007 Standard Edition určenou pro malé a střední společnosti.

Nyní, máme-li splněné všechny HW a SW požadavky přistoupíme k instalaci s využitím grafického průvodce nebo spuštěním bezobslužné instalace z příkazového řádku.

Grafický průvodce

Grafického průvodce spustíme pomocí souboru Setup.exe, který se nachází na instalačním mediu Exchange Server 2007 či v instalačním adresáři.

Po spuštění instalace se objeví zaváděcí obrazovka (Obr.17: Instalace - Bootstrapper), která nás informuje o stavu instalovaných komponent. Pokud jsou správně nainstalované, pak jsou příslušné odkazy neaktivní. V opačném případě musíme potřebný software doinstalovat. V našem případě máme aktivní až krok 5 - Instalaci Microsoft Exchange Serveru 2007, tedy můžeme pokračovat.

Následuje úvodní stránka s představením softwaru, který instalujeme (Obr.18: Instalace - Introduction).

Dále je nutné odsouhlasit zobrazené licenční ujednání EULA (Obr.19: Instalace - License Agreement).

Další stránka nám umožní zapnout automatické odesílání chybových hlášení pro Microsoft (Obr.20: Instalace - Error Reporting).

Na následující stránce vybíráme typ instalace a cestu pro instalaci softwaru. Volba „Typical Exchange Server Installation“ nainstaluje tři základní role, resp. čtyři role (Hub Transport, Mailbox, Client Access a nástroje pro správu Management Tool) na jeden server. Volba „Custom Exchange Server Installation“ se používá pokud potřebujeme instalovat určité vybrané role, např. při instalaci Exchange Serveru na více fyzických serverů. Podle návrhu instalujeme potřebné role na jeden server, vybíráme typickou instalaci (Obr.21: Instalace - Installation Type).

Zadáme jméno nové Exchange organizace. Pokud bychom prováděli instalaci do již vytvořené Exchange organizace, tato stránka se neobjeví (Obr.24: Instalace - Exchange Organization).

V další stránce rozhodneme, zda se v organizaci používá klient Outlook 2003 nebo dřívější. Z definovaných požadavků společnosti víme, že podporován bude Outlook 2007. Proto ponecháme výchozí nastavení. Tato volba je nutná z důvodu odlišnosti získávání informací o dostupnosti uživatelů podle kalendářových záznamů. Dříve se tyto informace získávali z databáze veřejných složek, kterou bychom museli rovněž v poštovním systému vytvořit. Od Exchange Serveru 2007 se potřebné informace získávají prostřednictvím webové služby Availability, která běží na CAS serveru (Obr.25: Instalace - Client Settings).

Opět proběhne prověření zda je systém k připraven k instalaci. Tentokráte prověření probíhá zvlášť pro každou serverovou roli. Pokud se objeví nějaká nesrovnalost, zobrazí se varovná hláška, příp. odkaz na podrobnější vysvětlení na webových stránkách

Microsoftu (Obr.26: Instalace - Readiness Checks).

Na další stránce sledujeme probíhající instalaci (Obr.27: Instalace - Progress).

Poslední stránka grafického průvodce informuje o provedené instalaci, úspěšných i neúspěšných krocích. V případě výskytu chyb v průběhu instalace jsou jejich příčiny zaznamenány také do Event Logu (Obr.28: Instalace - Completion).

Instalace je zakončena spuštěním EMC konzole a zobrazením doporučených a nepovinných kroků pro konfiguraci a vyladění poštovního systému (Obr.29: Instalace - EMC Finalize Deployment, Obr.30: Instalace - EMC End-to-End Scenario).

Úspěšnost instalace můžeme prověřit kontrolou Event Logu, kontrolou instalačních logů ExchangeSetup.log a ExchangeSetup.msilog v kořenovém adresáři ExchangeSetupLogs na systémovém disku, a také kontrolou, zda jsou automaticky spuštěny potřebné služby Microsoft Exchange.

Bezobslužná instalace

Další způsob, jak provést Instalaci Exchange Serveru 2007, je spuštění instalace z příkazového řádku.

Spustíme příkazový řádek cmd.exe.

Přepneme se na instalační médium, resp. do adresáře s instalačními soubory.

Spustíme příkaz Setup s parametry odpovídající požadované instalaci.

Následující příkaz ukazuje spuštění instalace pro role HT – Hub Transport, CA – Client Access, MB – Mailbox a MT – Management Tool, pro Exchange organizaci s názvem "MyOrganization".

Setup /mode:Install /roles:HT,CA,MB,MT /on:MyOrganization

Pokud porovnáme příkaz s instalací pomocí průvodce, zjistíme, že jsme ušetřeni některých voleb. Automaticky se předpokládá souhlas s licenčním ujednáním, neodesílání chybových hlášení pro Microsoft či využívání klientů Outlook 2007 pro přístup k mailboxům.

3.2 Střední společnost

3.2.1 Model

Popis

Společnost poskytuje finanční služby a poradenství na území celé České republiky. Hlavní sídlo společnosti je v Praze, pobočka v Ostravě. Celkem je zde zaměstnáno 1500 zaměstnanců. Každý zaměstnanec má přidělené stálé zákazníky. Podstatná část e-mailové komunikace se zákazníky je prováděna v pracovní době (Po-Pá 7:00-15:00). Dále pak dle potřeb zákazníka i mimo uvedenou pracovní dobu.

V hlavním sídle, v Praze, pracuje 1000 zaměstnanců.
Dalších 500 zaměstnanců pracuje v pobočce Ostrava.

V současnosti společnost využívá Hosted Exchange. Přístup k mailboxům je umožněn přes MS Outlook 2003 protokolem RPCoverHTTPs a pomocí Outlook Web Access. Nyní se společnost rozhodla přejít k implementaci vlastního elektronického poštovního systému. Potřebná data budou exportována do PST souborů a následně importována do nového systému pomocí klienta MS Outlook 2007.

Současný stav sítě

- Společnost má existující počítačovou síť s adresářovou strukturou Active Directory
- Hlavní sídlo i pobočka má samostatnou AD site s Domain Controllerem
- Každý Domain Controller je zároveň Global Catalog serverem
- Připojení k internetu je v místě hlavního sídla
- V místě internetového připojení je zřízen perimeter s firewallem
- Hlavní sídlo a pobočka jsou připojeny pomocí WAN 256Kbps
- Administrace sítě je řízena centrálně. Centrální administrátoři sídlí v Praze
- Na pobočce je lokální administrátor, který se stará o účty a podporu lokálních uživatelů
- Všichni zaměstnanci mají uživatelské účty v AD

Požadavky

- všechny příchozí zprávy musí projít antivirovou a antispamovou kontrolou
- centrální administrátoři budou odpovědni za správu a konfiguraci Exchange Serveru

- administrátor na pobočce bude vytvářet a konfigurovat účty lokálním uživatelům
- porucha Exchange Serveru bude mít minimální vliv na přístup k mailboxům
- v případě poškození Exchange databáze musí být možná obnova dat
- přístup k mailboxu musí být umožněn z interní i externí sítě
- pro přístup k mailboxu bude používán MS Outlook 2007 nebo webové rozhraní
- pro skupinu cca 50 pracovníků bude zřízen mobilní přístup (Exchange ActiveSync)
- pro publikaci Exchange služeb do Internetu bude využit MS ISA 2006 Server

3.2.2 Návrh infrastruktury

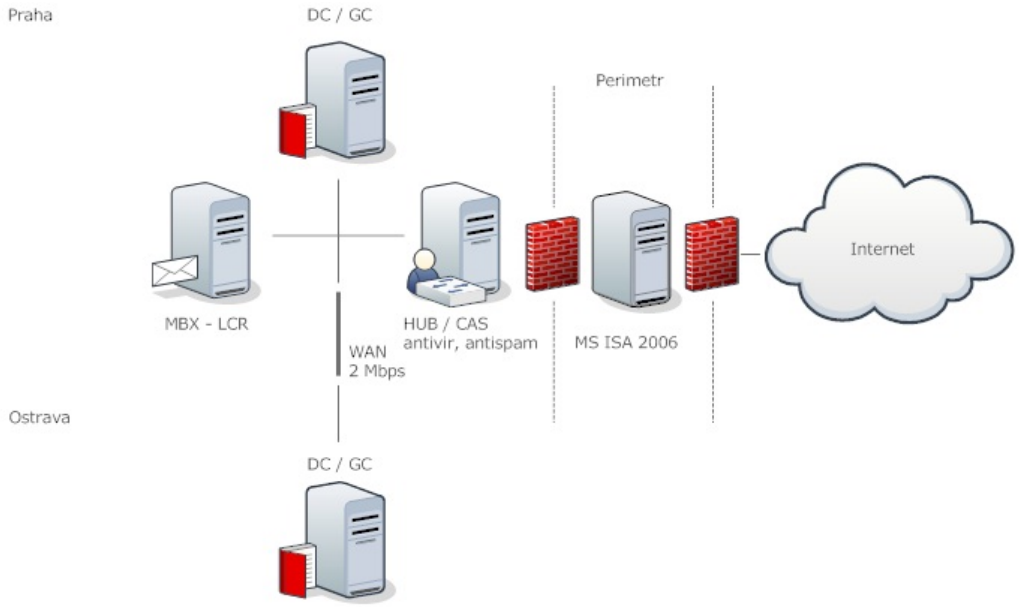
Pro návrh infrastruktury střední společnosti, která není soustředěna do jedné místní lokace, se nabízí více variant řešení. Proto navrhnu a popíši několik možností. Vyberu optimální řešení, které doplním o návod k instalaci. Při vytváření infrastruktury budu vycházet z možností, jenž nabízí Exchange Server 2007 Standard Edition a Exchange Server 2007 Enterprise Edition.

Návrh č.1

Z popisu společnosti je patrné rozložení počítačové sítě do dvou propojených lokací. Pouze v místě hlavního sídla je zřízeno připojení k internetu a perimetr. To znamená, že hlavní pobočkou musí procházet veškerá komunikace, příchozí i odchozí. V prvním návrhu budu vycházet z minimálního počtu fyzických serverů. Proto infrastruktura bude obsahovat jeden mailbox server, kde budou poštovní schránky všech 1500 zaměstnanců společnosti. Mailbox server bude umístěn v Praze, kde je internetové připojení.

K funkčnosti Exchange Serveru jsou nutné také serverové role CAS a Hub. Obě role budeme instalovat společně na druhý fyzický server. Oddělení role Mailbox nám sníží riziko dostupnosti poštovních schránek při havárií serveru s rolemi CAS a Hub. V tomto případě bude přístup k mailboxům umožněn alespoň pomocí MAPI klienta MS Outlook 2007 z vnitřní sítě, ačkoliv nebude možné přijímat a odesílat e-maily. Práce s obdobným omezením bude možná také pomocí klientů MS Outlook v režimu offline, kteří jsou nastaveni pro práci s mezipamětí (Cached Exchange Mode).

Pro případ poškození exchange databáze budeme na Mailbox server aplikovat funkci LCR. Jedná se o vytvoření kopie úložišť na další disk v rámci stejného serveru a udržování aktuálnosti dat pomocí průběžné replikace transakčních logů. Použití LCR zvyšuje nároky na paměť o 20% u serveru s rolí Mailbox. Zabezpečení dat pomocí LCR můžeme využít, v případě poškození dat databáze nebo při poruše pevného disku, k rychlému zprovoznění poštovního systému. Ovšem LCR neřeší situaci dalších možných příčin havárie fyzického serveru (pád OS, hardwarová závada, fyzické poškození).

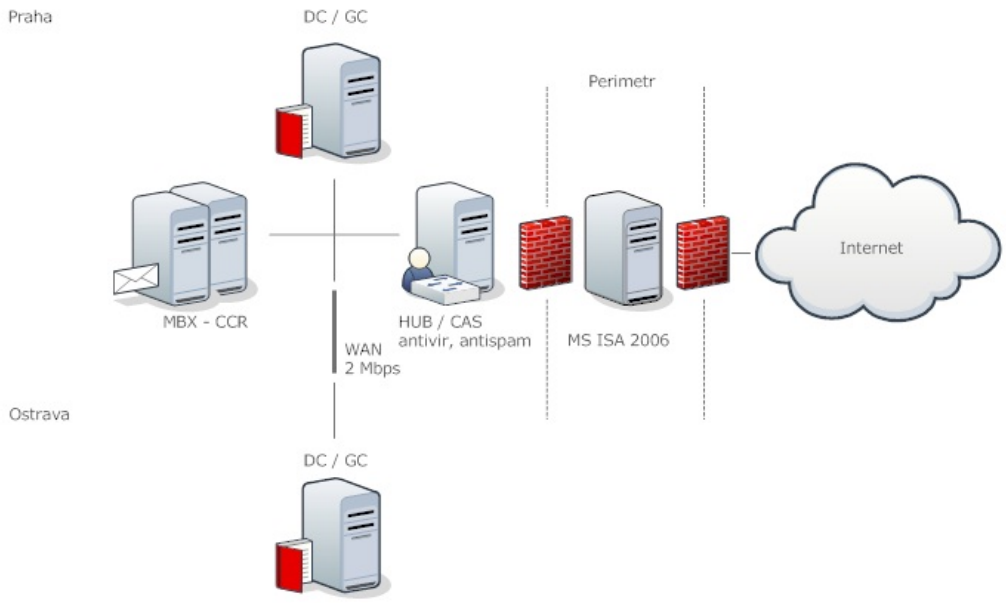


Obrázek 5: Střední společnost - Návrh Infrastruktury č.1

Podle požadavků bude pro publikaci Exchange služeb do Internetu využit MS ISA 2006 Server. Tento server umístíme do perimetru. Ve spojení s CAS serverem bude zajišťovat přístup k mailboxům z externí sítě pro klienty, webové rozhraní i mobilní přístup. Zároveň na tento server nasměrujeme MX záznamy pro příjem zpráv z internetu. Odchozí komunikace bude routována do internetu přímo.

Poslední co musíme navrhnout je umístění antivirové a antispamové ochrany. Jelikož MS ISA 2006 Server již tyto funkce neimplementuje, nasadíme na fyzický server s rolemi Exchange Server 2007 Hub a CAS antispamové agenty, kteří jsou určení k filtrování spamu pro serverovou roli Edge, příp. Hub. Na stejný fyzický server implementujeme Forefront Security for Exchange Server - antivirový software společnosti Microsoft.

Zaměstnanci z pobočky v Ostravě se budou připojovat ke svým poštovním schránkám umístěným na pražském Exchange Serveru prostřednictvím klienta MS Outlook 2007. Z tohoto důvodu je potřeba ověřit dostatečnost stávajícího připojení WAN 256 Kbps. Využijeme produkt Microsoft Systém Center Capacity Planer 2007, kde máme možnost simulace navrhované infrastruktury včetně zohlednění používaných klientů a hardwarového vybavení. Výsledkem simulace je nutnost navýšení kapacity připojení na 1Mbps pouze pro připojování se k Exchange Serveru klienty MS Outlook využívající Cached Exchange Mode. Jelikož v Ostravě není zřízeno připojení k internetu, bude i tato komunikace procházet WAN linkou. Kapacitu linky WAN mezi Prahou a Ostravou navýšíme na 2Mbps. Pro licenční pokrytí infrastruktury postačí zakoupení Exchange Server 2007 Standard Edition.



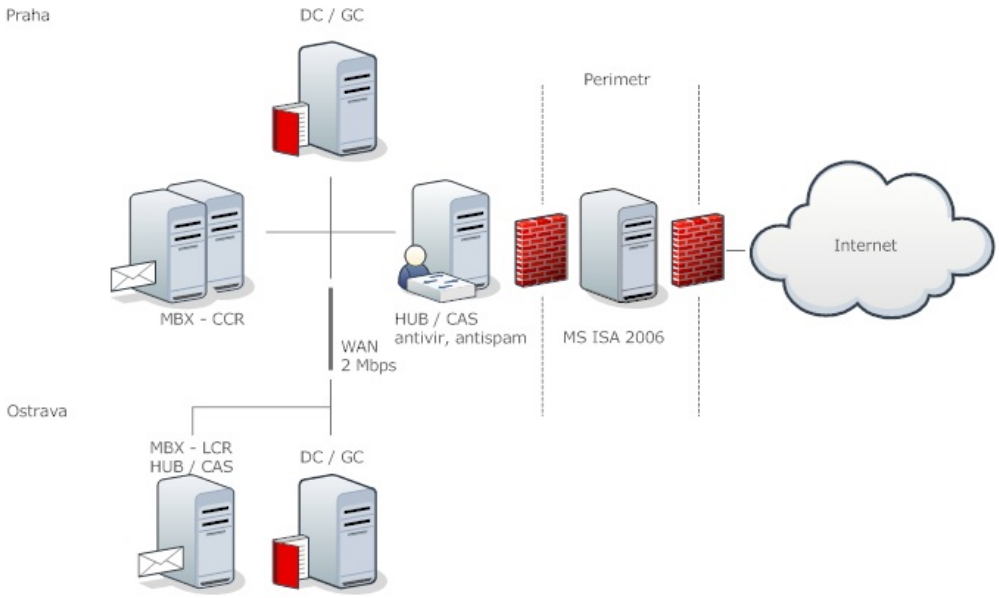
Obrázek 6: Střední společnost - Návrh Infrastruktury č.2

Návrh č.2

Druhý návrh bude prakticky totožný s prvním. K vylepšení dojde pouze v oblasti vysoké dostupnosti, kde zaměníme LCR za CCR. CCR vytváří kopii úložišť na další samostatně stojící server. To znamená, že původní infrastruktura (z 1.návrhu) bude rozšířena o další fyzický server.

Cluster Continuous Replication využívá technologii zapojení dvou serverů v clusteru typu aktivní – pasivní. Průběžnou replikací transakčních logů z aktivního uzlu na pasivní se udržuje aktuální stav databáze na pasivním uzlu. Navíc CCR podporuje automatický failover (převzetí služeb) v případě havárie aktivního uzlu. Automatický přechod na kopii pasivní skupiny úložišť je pro CCR výhodou oproti řešení využívající LCR, kde je k přechodu na pasivní kopii nutný zásah administrátora. Při implementaci zabezpečení vysoké dostupnosti pomocí CCR již musíme použít Enterprise edice pro Exchange Server 2007 a také pro Windows Server 2003 nebo 2008.

Pokud by pro společnost, v případě selhání serveru s rolemi Hub a CAS, nebyla dostačující dočasná dostupnost mailboxu pouze z vnitřní sítě pomocí MS Outlooku (pro čtení doručené pošty a přípravy zpráv k odeslání) bez další obvyklé funkčnosti jako je doručování zpráv či využívání webových služeb, zahrnuli bychom do infrastruktury další fyzický server, který by opět implementoval obě role Hub, CAS a prvky pro antivirovou a antispamovou ochranu.



Obrázek 7: Střední společnost - Návrh Infrastruktury č.3

Pro práci zaměstnanců je nutný přístup k doručené poště. Tuto postupně zpracovávají, vyřizují požadavky telefonicky, kompletují tištěné dokumenty, atd. Proto je vyjímečný krátkodobý výpadek služeb zajišťovaných serverovými rolemi Hub a CAS přípustný. V návrhu poštovního systému společnosti ponecháme pouze jeden fyzický server se zmíněnými rolemi. Případný dlouhodobý výpadek bude řešen dle aktuální situace a havarijního plánu společnosti. Nabízí se možnosti od dočasné instalace Hub a CAS role na DC nebo jiný vyhovující server ve společnosti, až po instalaci nového serveru.

Návrh č.3

Exchange Server 2007 díky nové architektuře založené na serverových rolích umožňuje vytvářet množství různých typů návrhu infrastruktury vedoucí k řešení stejných požadavků. Opět provedeme malou modifikaci předchozího návrhu a vytvoříme novou infrastrukturu, ve které zohledníme možnost vybudování vlastního Exchange Serveru na pobočce v Ostravě.

V Praze zachováme kompletní infrastrukturu z 2.návrhu. Zaměstnanci hlavního sídla budou mít umístěny poštovní schránky na Mailbox serveru v Praze a vysoká dostupnost mailboxů bude zabezpečena pomocí CCR. Serverové role Hub a CAS budou instalované na samostatně stojícím serveru, na kterém bude také prováděna antispamová a antivirová kontrola. V místě perimetru bude instalovaný ISA Server 2006 pro přístup k mailboxům z externí sítě. Na ISA Server budou nasměrovány MX záznamy pro příjem pošty z internetu.

Ostravští zaměstnanci budou mít poštovní schránky na vlastním Mailbox serveru. Na ostravskou pobočku přidáme fyzický server pro instalaci Exchange serveru s rolí Mailbox. Protože ke své funkčnosti potřebuje Exchange Server mimo Mailboxu opět role CAS a Hub, přidáme tyto role na stejný fyzický server.

Zbývá vyřešit zabezpečení dat na Mailbox serveru v Ostravě. Jelikož se jedná o jeden fyzický server budeme aplikovat funkce LCR popsané v 1.návrhu.

Pro licenční pokrytí této infrastruktury budeme potřebovat oba typy licencí. Exchange Server 2007 Standard Edition pro ostravskou pobočku a pražský server s rolemi CAS a Hub. Exchange Server 2007 Enterprise Edition s Enterprise edicí Windows Serveru pro fyzické servery s rolemi Mailbox instalované v Praze.

3.2.3 Instalace Exchange Serveru 2007

Pro popis instalace Exchange serveru 2007 ve střední společnosti vybereme návrh č.2. Hlavní výhodou je způsob zabezpečení vysoké dostupnosti pomoci CCR s funkcí automatického převzetí služeb. Centralizace zdrojů nám vzhledem k celkovému počtu mailboxů, které lze umístit na jeden CMS server, umožní nezvyšovat náklady nutné při případné instalací Exchange Serveru na ostravské pobočce.

K implementaci elektronického poštovního systému společnosti Microsoft budeme potřebovat 3 fyzické servery pro Exchange Server 2007 a 1 fyzický server pro instalaci MS ISA Serveru 2006, který bude umístěn v perimetru. Instalací a konfigurací ISA Serveru se nebudeme zabývat, jelikož by se jednalo o včlenění dalších obsáhlých kapitol, které nejsou náplní práce.

Fyzický server, který bude plnit funkci serverových rolí Hub a CAS opatříme OS Windows Server Standard Edition 2003 nebo 2008. Na oba servery určené pro role Mailbox se zabezpečením vysoké dostupnosti pomocí CCR nainstalujeme Enterprise edici serverového operačního systému Windows Server 2003 nebo 2008. Všechny servery připravíme dle přílohy Příprava k instalaci Exchange Serveru 2007. V případě serveru s kumulovanými rolemi CAS a Hub budeme na server aplikovat soubor požadovaných prvků pro obě role.

Servery, na které budeme instalovat serverové role Clustered Mailbox, nachystáme podle stručného návodu k vytvoření Windows Clusteru pro CCR, jenž je uveden ve stejnojmenné příloze.

Jestliže jsou servery připraveny, zahájíme instalaci Exchange Serveru 2007. V infrastrukturách, kde je Exchange Server instalován na více fyzických serverů je nutné jako první nainstalovat serverovou roli CAS. Z tohoto důvodu budeme nejprve instalovat fyzický server s rolemi CAS a Hub. V dalším kroku nainstalujeme servery s rolemi Clustered Mailbox. Na závěr opatříme systém antispamovou a antivirovou ochranou.

Grafický průvodce

Některé obrázky použité pro názornost prováděné instalace pomocí grafického průvodce, jsou společné pro všechny typy instalací, proto se mohou nepatrně lišit. Odlišnosti jsou zejména ve výčtu vybraných serverových rolí.

Instalace role HUB a CAS

Na fyzickém serveru se Standard edicí serverového operačního systému Windows vyhledáme v instalačním adresáři Exchange Server 2007 soubor Setup.exe, kterým spustíme Grafického průvodce.

Na zaváděcí obrazovce zkontrolujeme stav instalovaných komponent. Jsou-li všechny požadavky splněny, pokračujeme v instalaci. (Obr.17: Instalace - Bootstrapper)

Přes stránky informující o instalovaném softwaru (Obr.18: Instalace - Introduction), licenčním ujednání EULA (Obr.19: Instalace - License Agreement) a odesílání chybových hlášení z průběhu instalace (Obr.20: Instalace - Error Reporting) se přeneseme k výběru typu instalace (Obr.21: Instalace - Installation Type).

Zvolíme „Custom Exchange Server Installation“ a následně vybereme k instalaci role CAS a Hub (Obr.22: Instalace - Server Role Selection). Automaticky bude nainstalován i Management Tools pro správu systému.

Zadáme jméno nové Exchange organizace (Obr.24: Instalace - Exchange Organization).

Stránku s výběrem verze Outlook klienta necháme beze změn (Obr.25: Instalace - Client Settings)

Po prověření připravenosti k instalaci dle zvolených serverových rolí (Obr.26: Instalace - Readiness Checks) můžeme sledovat probíhající instalaci (Obr.27: Instalace - Progress.)

Na závěr jsme informování o výsledku instalace (Obr.28: Instalace - Completion).

Po spuštění EMC konzole se zobrazí seznam doporučených kroků k doladění instalace Exchange Serveru 2007 (Obr.29: Instalace - EMC Finalize Deployment , Obr.30: Instalace - EMC End-to-End Scenario).

Instalace role Mailbox - CCR

Pro instalaci Mailbox serveru s vysokou dostupnosti CCR potřebujeme právě dva fyzické servery, které jsou uzly Windows Clusteru. Instalaci Exchange uskutečníme nejprve pro aktivní uzel a celý postup zopakujeme pro instalaci pasivního uzlu clusteru.

Na požadovaném Mailbox serveru (aktivní/pasivní uzel) spustíme z instalačního adresáře Grafického průvodce instalací Exchange Serveru 2007.

Přes zaváděcí a informativní stránky přejdeme k výběru typu instalace (Obr.21: Instalace - Installation Type).
Zvolíme „Custom Exchange Server Installation“ a označíme instalaci Active Clustered Mailbox Role (Obr.22: Instalace - Server Role Selection).

Na stránce s nastavením clusteru vybereme typ zabezpečení vysoké dostupnosti Cluster Continuous Replication, specifikujeme jméno Mailbox Serveru a přístupovou IP adresu. Cestu k databázovému úložišti a k transakčním logům můžeme ponechat ve výchozím nastavení. Pokud však máme možnost ukládat transakční logy na jiný disk serveru, provedeme příslušnou změnu v nastavení cesty (Obr.23: Instalace - Cluster Settings).

Následuje prověření připravenosti k instalaci (Obr.26: Instalace - Readiness Checks) a pokud je vše v pořádku je instalace spuštěna. O průběhu instalace a úspěšném výsledku, příp. vzniklých chybách jsme informováni na stránkách Progress Obr.27 a Completion Obr.28.

Bezobslužná instalace

Instalaci Exchange Serveru 2007 z příkazového řádku provedeme ve shodném pořadí jako tomu bylo u instalace s grafickým průvodcem. Nejprve nainstalujeme fyzický server s rolí Hub a CAS. Následovat bude instalace Aktivního a Pasivního uzlu Mailbox clusteru.

Na serverech, které budeme postupně instalovat, se v příkazovém řádku přepneme do instalačního adresáře Exchange Serveru 2007.

Pro instalací rolí Hub a CAS použijeme příkaz :

Setup /mode:Install /roles:HT,CA,MT /on:MyOrganization

Active Clustered Mailbox Roli zprovozníme ve dvou krocích – instalací Binárních dat Exchange Serveru a vytvořením clusteru :

Setup /mode:Install /roles:MB,MT
Setup /NewCMS /CmsIpAddress:192.168.1.10 /CmsName:E2K7CCR

Instalaci role Pasive Clustered Mailbox provedeme příkazem :

Setup /mode:Install /roles:MB,MT

Instalace funkcí antispamu

Máme-li úspěšně nainstalovány potřebné role k provozování Exchange Serveru 2007 můžeme přistoupit k instalaci antispamových agentů. Funkce antispamu jsou součástí instalace Exchange Serveru 2007 a běžně se instalují se serverovou rolí Edge Transport. V naší infrastruktuře není serverová role Edge Transport obsazena, proto nainstalujeme funkce antispamu pomocí příkazů PowerShelu přímo na server s rolí Hub.

1. Administrátorským účtem se přihlásíme pomocí RDP klienta na Exchange Server s rolí Hub.

2. Pokud je spuštěna Exchange Management Console, ukončíme ji.

3. Spustíme Exchange Management Shell.

4. Přepneme se do adresáře Scripts

cd "C:\Program Files\Microsoft\Exchange Server\Scripts"

5. Spustíme instalační script (Obr.31: Antispam - Spuštění Scriptu):

./ install-AntispamAgents.ps1

6. Pro aplikaci změn je nutný restart služby Microsooft Exchange Transport. Restart provedeme v grafickém rozhraní pro správu služeb, spuštěním services.msc nebo příkazy PowerShellu (Obr.32: Antispam - Restart Služby) :

Stop-Service MSExchangeTransport
Start-Service MSExchangeTransport

7. V EMC konzoli se přemístíme v navigačním stromu na Organization configuration list\ Hub Transport. V pravé části okna, na záložce Anti-Spam, můžeme nastavovat jednotlivé antispamové filtry (Obr.33: Antispam - EMC Filtering)

Instalace Microsoft Forefront Security for Exchange Server

Na úvodní obrazovce grafického průvodce instalací Exchange Serveru 2007 je hypertextový odkaz, který nás nasměruje na stránky Microsoftu, kde je možné si produkt stáhnout (Obr.17: Instalace - Bootstrapper). Máme-li instalační software k dispozici, přistoupíme k instalaci. Přihlásíme se na server, na který chceme MS Forefront Security for Exchange Server instalovat. V našem případě se jedná o server s rolí Hub. Instalační průvodce se nachází v příloze Instalace Forefront Security for Exchange Server.

3.3 Velká společnost

3.3.1 Model

Popis

Společnost zabývající se poskytováním služeb a řešení v oblasti informačních technologií. Jedná se o centrálně řízenou společnost zaměstnávající 5000 zaměstnanců. Společnost má hlavní sídlo a 40 poboček po celém světě. Služby jsou s ohledem na časové zóny poskytovány nepřetržitě. Pro společnost je kritická vysoká dostupnost služeb elektronického poštovního systému.

Počty zaměstnanců v hlavním sídle a na pobočkách se výrazně neliší.
Žádná pobočka, ani hlavní sídlo, nemá víc než 150 zaměstnanců.

Společnost vznikala postupným slučováním menších firem. Každá pobočka využívala jiný typ e-mailového systému. Implementace MS Exchange Serveru 2007 ve společnosti je řešení pro zavedení jednotnosti a umožnění centrální správy e-mailového systému.

Současný stav sítě

- Společnost má již nově vybudovanou síťovou infrastrukturu s AD strukturou
- Ta zahrnuje 1 HQ - hlavní sídlo a 8 regionálních center
- Každé RC má připojený určitý počet poboček WAN linkou 128 Kbps
- Regionální centra jsou spojena s HQ linkami WAN 2Mbps
- Každá fyzická část struktury AD má vlastní AD site, v které je Domain Controller
- Domain Controllery v HQ a RC jsou konfigurovány jako Global Catalog servery
- Na pobočkách jsou DC s aktivní funkci UGMC
- Hlavní sídlo má vysokorychlostní připojení k internetu
- V místě internetového připojení je zřízen perimeter
- Připojení k internetu je zřízeno také ve všech regionálních centrech a pobočkách
- Podporované protokoly v síti jsou MAPI, HTTP-S, SMTP
- Každý uživatel má vytvořený účet v AD

Požadavky

- všichni uživatelé budou využívat plný přístup ke všem službám exchange serveru
- přístup k mailboxu bude umožněn z interní i externí sítě

- používaní klienti : MS Outlook a webové rozhraní
- správa a konfigurace exchange serveru bude řízena centrálně, týmem administrátorů
- příchozí i odchozí zprávy budou procházet antivirovou a antispamovou kontrolou
- DNS MX záznamy směřují na SMTP bránu v sídle společnosti
- počty nově instalovaných serverů budou minimální
- v případě poškození databáze musí být možná rychlá obnova dat
- e-mailový systém musí být dostupný i v čase údržby systému
- přístup přes webové rozhraní musí zajišťovat alespoň dva servery
- webové rozhraní bude požadovat zabezpečený přístup

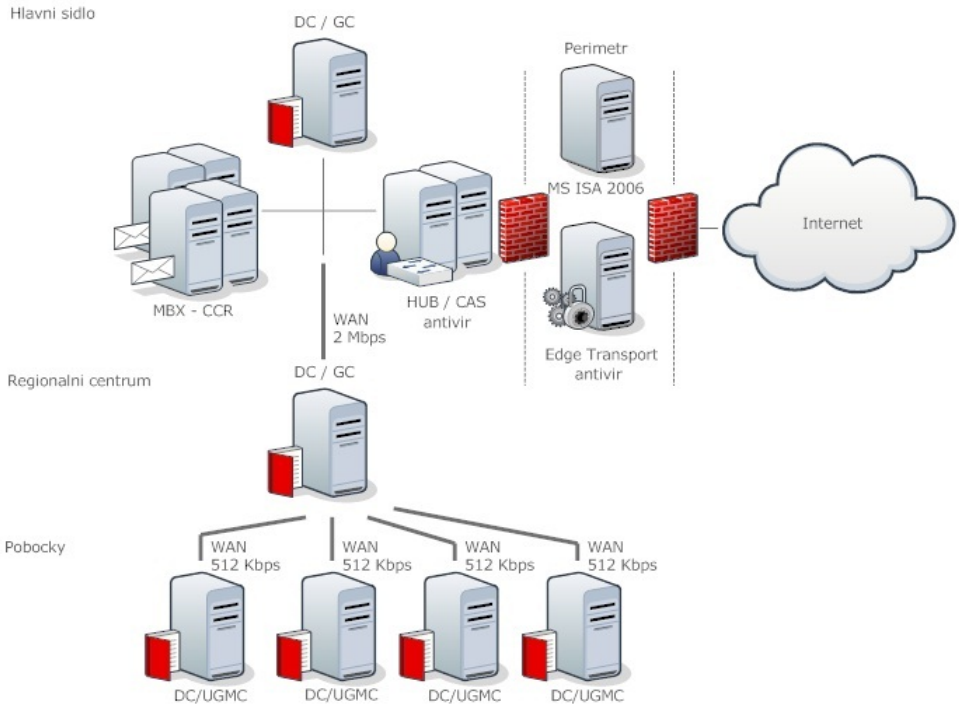
3.3.2 Návrh infrastruktury

Společnost s hlavním sídlem, 8 regionálními centry a dalšími pobočkami náležícími k regionálním centrům představuje rozsáhlou síťovou infrastrukturu. Počet připojených poboček je poměrně vysoký, takže o umísťování Exchange Serverů na koncové pobočky nebudeme vzhledem k minimálním počtům nově instalovaných serverů uvažovat.

V požadavcích organizace je kladen velký důraz na vysokou dostupnost poštovního systému, proto budeme ve všech návrzích využívat možnosti zálohování nabízené prostřednictvím Exchange Server 2007 Enterprise Edition. Ve snaze o zavedení jednotnosti poštovního systému a jeho zapojení bude všech 8 větví, jimiž jsou k HQ připojena regionální centra a jejich pobočky, řešeno identickým způsobem. Graficky vyjádřené návrhy pak budou zobrazovat vzorové připojení jedné takovéto větve.

Návrh č.1

Společnost zahrnuje 40 lokalit propojených přímo nebo prostřednictvím regionálního centra s hlavním sídlem. V HQ je zřízen perimetr a vysokorychlostní připojení k internetu, které využívají všechny zmíněné lokality pro výměnu zpráv směrovaných z internetu do společnosti a opačně.



Obrázek 8: Velká společnost - Návrh Infrastruktury č.1

Návrh poštovní infrastruktury pro centrálně řízenou společnost zahájíme umístěním serverové role Mailbox do HQ, kde budou uloženy poštovní schránky všech uživatelů společnosti. Pro umístění 5000 mailboxů budeme potřebovat dva, resp. čtyři fyzické servery, na které budeme aplikovat funkce CCR z důvodu požadavku vysoké dostupnosti systému.

Dalším požadavkem je zajištění přístupu přes webové rozhraní alespoň dvěmi servery. Tato služba je zprostředkována serverovou rolí CAS. Vybudujeme tedy další dva fyzické servery pro instalaci role Client Access Server.

Serverovou roli Hub nutnou pro funkčnost Exchange Serveru implementujeme na oba fyzické servery s rolí CAS. Exchange Server 2007 umožňuje obě role instalovat na jeden fyzický server. Aplikací serverové role Hub na oba servery, snížíme riziko nefunkčnosti doručování e-mailů vzniklé případným selháním serveru s jmenovanou rolí. Na servery aplikujeme technologii vyrovnání zatížení sítě Windows NLB.

Zabezpečený přístup k poštovním schránkám přes webové rozhraní zajistíme na obou serverech s rolí CAS instalací SSL certifikátu. Z důvodu zvýšení bezpečnosti budeme pro publikaci exchange služeb do Internetu využívat MS ISA 2006 Server, který umístíme do

perimetru. To nám umožní provádět autentizaci uživatelů přistupujících z externí sítě ještě dříve než se připojí na CAS ve vnitřní síti společnosti.

Příchozí i odchozí komunikace bude procházet antivirovou a antispamovou kontrolou. Za tímto účelem postavíme samostatný fyzický server se serverovou rolí Edge Transport. Server umístíme rovněž do perimetru a nasměrujeme na něj MX záznamy pro příjem pošty z internetu. Silnou antivirovou ochranu zajistíme instalací Forefront Security for Exchange Server jak na Edge Transport tak i na oba Hub Transport Servery společnosti.

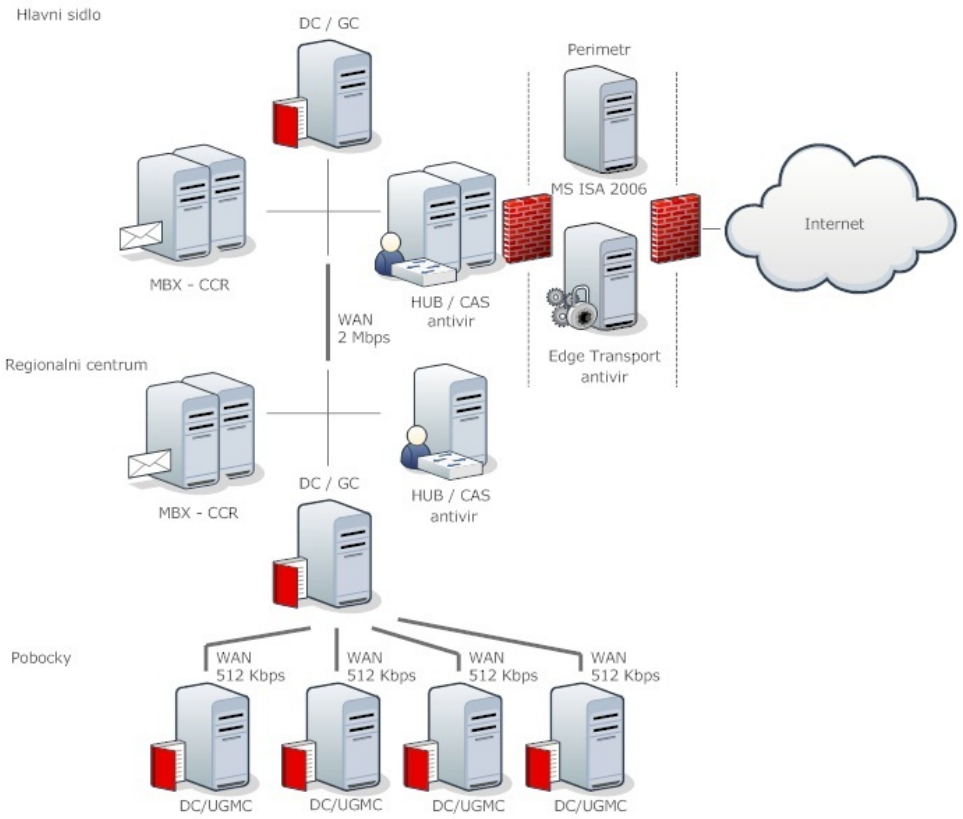
Regionální centra i pobočky mají zřízené vlastní internetové připojení pro přístup k internetu. WAN linky mezi HQ , RC a pobočkami budou využívány především pro RPC komunikaci pomocí protokolu TCP/IP. Dostatečnost kapacity WAN linek prověříme pomocí nástroje Systém Center Capacity Planer 2007. Spojení HQ a jednoho regionálního centra bude využívat 500 – 700 uživatelů. WAN linku mezi RC a jednou pobočkou je určeno pro maximálně 150 uživatelů. Pro připojení koncových poboček s regionálními centry je nutné navýšit kapacitu WAN linky na 512 Kbps. Mezi HQ a jednotlivými RC jsou 2 Mbps dostačující.

Návrh č.2

Nyní se podíváme, jak by vypadal návrh, kde bychom chtěli Mailbox servery přesunout blíže k uživatelům pracujícím v RC a koncových pobočkách. To znamená, že bychom servery s rolí Mailbox včetně zajištění vysoké dostupnosti pomocí CCR, které lze považovat za nejspolehlivější ve všech ohledech z nabízených řešení Exchange Serveru 2007, umístili nejen do HQ, ale také do všech regionálních center.

Již v tuto chvíli lze odhadnout, že řešení nesplňuje požadavek na minimální počet nově instalovaných serverů. Ke každé dvojici mailbox serverů bychom museli přidat další fyzický server s rolemi CAS a Hub, takže v každém z osmi regionálních center přibudou tři nové servery.

Při zachování myšlenky Mailbox serverů umístěných v regionálních centrech bychom mohli snížit počet nových serverů až na jeden. Tzn. na jeden fyzický server bychom instalovali společně základní role MBX, CAS a Hub se zabezpečením vysoké dostupnosti pomocí funkce LCR. Toto řešení by však zvýšilo riziko nedostupnosti systému vzniklé selháním systému, což je pro tuto společnost nepřijatelné.

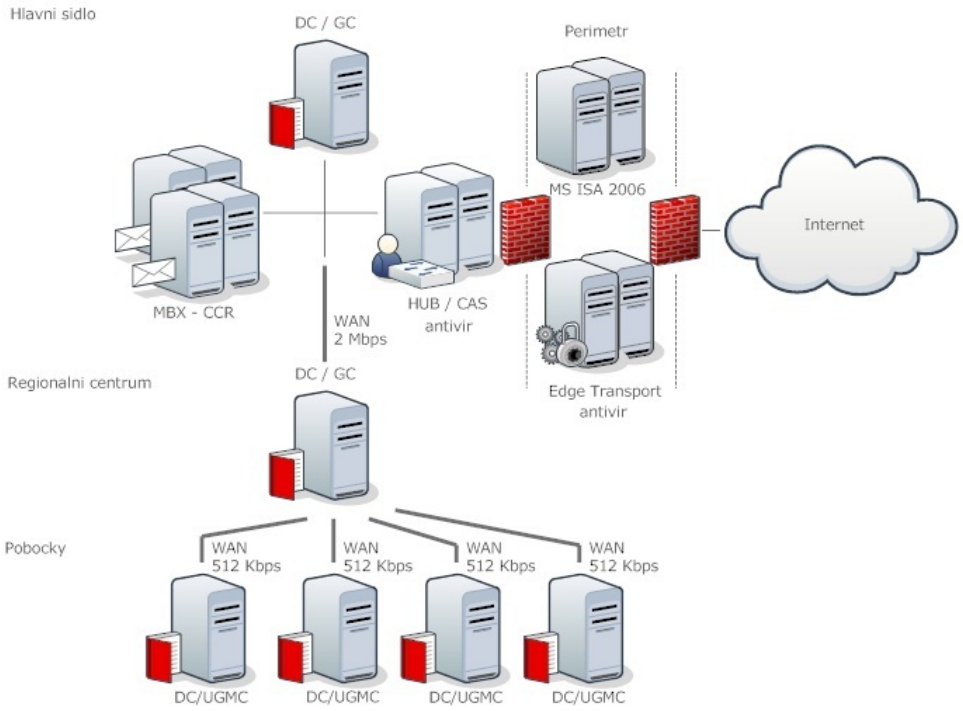


Obrázek 9: Velká společnost - Návrh Infrastruktury č.2

Návrh č.3

Vzhledem k ne zcela optimálnímu předchozímu návrhu upustíme od možnosti přesouvání serverů s rolí Mailbox do regionálních center a vrátíme se k prvnímu centralizovanému návrhu. V hlavním sídle máme čtyři Mailbox servery včetně zajištění vysoké dostupnosti CCR a dva servery se sloučenými rolemi CAS a Hub.

Jediné místo, které zůstalo nezabezpečeno z pohledu možné havárie je nyní Edge Transport a ISA Server v perimetru. Jelikož je vysoká dostupnost služeb elektronického poštovního pro společnost velmi důležitá, posílíme perimetr o další servery s rolí Edge Transport a ISA Server 2006. Rozložení zátěže pro oba typy serveru bude zajišťovat hardwarový load-balancer. MX záznamy rozšíříme o směrování pošty také na nový Edge Transport server.



Obrázek 10: Velká společnost - Návrh Infrastruktury č.3

3.3.3 Instalace Exchange Serveru 2007

Z třetího návrhu implementace Exchange Serveru 2007 je patrné, že nejlépe odpovídá požadavkům modelu velké společnosti. Umístění všech serverů s rolemi Exchange Serveru do HQ vyhovuje centrální správě i minimalizaci zdrojů. Clusterované Mailbox role společně s dvěmi servery CAS/Hub splňují nároky na vysokou dostupnost systému. Přidáním serverů ISA a Edge Transport jsme odstranili poslední možná slabá místa - SpoF.

Realizace návrhu bude spočívat v instalaci 10 fyzických serverů. My se budeme zabývat pouze servery, které jsou určené pro instalaci Exchange Serveru 2007. Z grafického návrhu je zřejmé, že se jedná o servery s rolemi Mailbox, CAS, Hub a Edge Transport. Všechny servery, vyjma Edge Transport Serveru, budou připojeny k interní síti a budou součástí struktury služby AD. Edge Transport bude umístěn do perimetru.

Před spuštěním vlastní instalace připravíme všechny budoucí Exchange servery podle přílohy Příprava k instalaci Exchange Serveru 2007. Pro každé dva Mailbox Servery vytvoříme samostatný Windows Cluster, viz. příloha Vytvoření Windows Clusteru.

Mimořádnou pozornost budeme věnovat přípravě Edge Transport Serveru, který se poprvé objevuje až v návrhu infrastruktury velké společnosti. To neznamená, že by roli Edge Transport nebylo možné implementovat do Exchange infrastruktury v malých a středně velkých společnostech. Důvodem neobsazenosti role bylo nasazení odlišných řešení ochrany proti spamu a virům. V malé společnosti byla hygiena zpráv řešena v rámci aplikačního firewallu. U střední společnosti se jednalo o nasazení antivirových a antispamových agentů určených pro Edge Transport, bez nutnosti instalace vlastní role Edge. Agenti byli instalovány na Exchange server s roli Hub.

Role Edge Transport zabezpečuje antispamové funkce, umožňuje sestavování transportních pravidel a směrování pomocí SMTP protokolu. Server je umístěn v perimetru a není součástí interní AD struktury. Data z AD jsou čerpána pomocí procesu EdgeSync. Údaje o příjemcích, bezpečných odesilatelích, interních doménách a další konfiguraci získané jednosměrnou replikací z AD se ukládají na Edge serveru do adresářové služby ADAM. Služba ADAM se spouští jako uživatelská služba a není závislá na DC.

Před instalací Exchange na Edge server je nutné na připraveném fyzickém stroji dle přílohy Příprava k instalaci Exchange Serveru 2007 vytvořit DNS příponu. Dále pro komunikaci Edge s Hub Transport servery musíme do lookup zóny na interním DNS serveru přidat záznam hostitele, tj. Edge server. A nezapomeneme na instalaci služby ADAM. Soubor instrukcí pro přípravu Edge Transport serveru včetně konfigurace, která se provede po nainstalování serverové role, zahrnuje příloha Edge Transport Server.

Nyní jsme připraveni k instalaci všech rolí Exchange Serveru. Nejprve nainstalujeme servery s rolí CAS/Hub, dále clusterované Mailbox role a jako poslední provedeme instalaci Edge Transport serveru.

Grafický průvodce

Instalace s využitím Grafického průvodce již byla popsaná v kapitole 3.2.3, kde byla řešena instalace Exchange Serveru pro společnost střední velikosti. Postupy a průběh instalace jsou pro všechny role shodné, včetně instalace Edge Transport serveru. Rozhodující je pouze zvolený typ instalace “Custom“ (Obr.21: Instalace - Installation Type) a výběr požadované role (Obr.22: Instalace - Server Role Selection).

Bezobslužná instalace

Instalaci z příkazového řádku lze rovněž snadno odvodit od návodu pro střední společnost. Na aktuálně instalovaném serveru se přepneme vždy do instalačního adresáře Exchange Serveru 2007 a budeme provádět příkazy :

EXCH-HUBCAS1 : **Setup /mode:Install /roles:HT,CA,MT /on:MyOrganization**

EXCH-HUBCAS2 : **Setup /mode:Install /roles:HT,CA,MT**

EXCH-CCR1M1: **Setup /mode:Install /roles:MB,MT**
Setup /NewCMS /CmsIpAddress:192.168.1.10 /CmsName:E2K7CCR1

EXCH-CCR1M2: **Setup /mode:Install /roles:MB,MT**

EXCH-CCR2M1: **Setup /mode:Install /roles:MB,MT**
Setup /NewCMS /CmsIpAddress:192.168.1.11 /CmsName:E2K7CCR2

EXCH-CCR2M2: **Setup /mode:Install /roles:MB,MT**

Edge Transport1: **Setup /mode:Install /roles:ET,MT**

Edge Transport2: **Setup /mode:Install /roles:ET,MT**

Instalace Microsoft Forefront Security for Exchange Server

Jestliže máme úspěšně nainstalován Exchange Server 2007 opatříme systém antivirovou ochranou. V libovolném pořadí nainstalujeme na servery s rolemi Hub a Edge transport produkt MS Forefront Security for Exchange Server. Průvodce instalací antiviru je popsán v příloze Instalace Forefront Security for Exchange Server.

4 Konfigurace a správa poštovních serverů s Microsoft Exchange 2007

V této části volně navážeme na předchozí kapitolu popisující instalace MS Exchange Serveru 2007 ve společnostech různých velikostí. Nebudeme se tedy zabývat úplnou konfigurací systému pro jednotlivé modelové příklady, ale ukážeme kroky, které ke konečné konfiguraci vedou. Pomocí grafického rozhraní i příkazového řádku předvedeme základní operace nutné pro správu elektronického poštovního systému společnosti Microsoft.

Předpokladem k zahájení konfigurace je úspěšně nainstalovaný poštovní server MS Exchange Serveru 2007, resp. potřebné role poštovního systému na požadovaném počtu fyzických serverů dle navržené infrastruktury. Po instalaci se poštovní systém nachází ve výchozím nastavení, které je třeba zkontrolovat popř. upravit dle individuálních potřeb společnosti.

Ke správě systému pomocí grafického uživatelského rozhraní využijeme EMC konzoli, která je zpravidla dostupná na každém fyzickém serveru s alespoň jednou instalovanou rolí MS Exchange Serveru 2007. EMC konzole (Obr.65: Konfigurace - EMC) je rozdělena na čtyři části. V levé části je navigační strom, jehož uzly seskupují serverové role podle typu správy – Konfigurace na úrovni organizace, Konfigurace serveru a Konfigurace příjemců. Poslední uzel Toolbox je vyhrazen pro sadu nástrojů. Střední část EMC tvoří podokno výsledků navigačního stromu a podokno pracovní. V pravé části je seznam aktuálně dostupných akcí. Zvolená akce je obvykle provázena spuštěním grafického průvodce, který před dokončením vypíše odpovídající příkaz Exchange Management Shellu.

Administraci z příkazového řádku budeme provádět v prostředí Exchange Management Shellu. Základní používané příkazy jsou Get, Set a New. Výpis dostupných parametrů určitého příkazu v případě potřeby uskutečníme pomocí Get-Help, např. Get-Help New-Database. Pro psaní resp. doplňování příkazů v EMS lze s výhodou využívat funkci PowerTab intellisense.
Nyní se podíváme na některá nastavení a konfiguraci jednotlivých serverových rolí.

4.1 Mailbox

Společnost libovolné velikosti má nově nainstalovaný poštovní systém MS Exchange Server 2007. Všichni zaměstnanci mají zřízené uživatelské účty v AD. Uživatelské mailboxy budou zahrnuty v poštovních databázích a každá databáze bude z důvodu snížení zátěže a větší flexibility při obnově, umístěna v jednom databázovém úložišti.

Počet databázových úložišť závisí na potřebách společnosti a je omezen pořízenou licencí. Pravidla, podle kterých budou zřizovány poštovní schránky uživatelů na určitých databázích závisí rovněž na potřebách společnosti. Samozřejmostí je snaha o rovnoměrné rozložení zátěže na všechny poštovní databáze.

Po instalaci serverové role Mailbox je automaticky vytvořena jedna skupina databázového úložiště s jednou připojenou databází poštovních schránek. Pokud by byla pro společnost jedna databáze dostačující, mohli bychom rovnou přistoupit k vytvoření mailboxů k uživatelským účtům. Tento stav je však méně častý, proto je obvykle nutné vytvořit potřebný počet skupin databázových úložišť a poštovních databází.

Založení skupiny úložišť
V navigačním stromu EMC vyhledáme uzel Server Configuration/Mailbox. V okně zobrazující seznam Mailbox serveru vybereme server, jehož úložiště budeme spravovat. V pracovním podokně jsou zobrazeny aktuální skupiny úložišť, jejich databáze a stav připojení (Mounted/Dismounted). Pro vytvoření nové skupiny úložišť zvolíme z panelu akcí New Storage Group (Obr.65: Konfigurace – EMC). Zobrazí se průvodce, kde vyplníme jméno nového úložiště, umístění systémových souborů a transakčních logů (Obr. 66: Konfigurace – New Storage Group). Po dokončení jsme informováni o úspěšném vytvoření nového úložiště.

Stejnou akci, provedeme pomocí EMS :
new-StorageGroup -Server "E2K7CCR" -Name "Second Storage Group" -LogFolderPath "C:\Program Files\Microsoft\Exchange Server\Mailbox\Second Storage Group" -SystemFolderPath "C:\Program Files\Microsoft\Exchange Server\Mailbox\Second Storage Group"

Založení databáze poštovních schránek
V pracovním podokně se přepneme na nově vytvořenou skupinu úložišť a zvolíme akci New Mailbox Databaze. Opět se spustí průvodce, kde zadáme jméno nové databáze, umístění databázového souboru a označíme volbu pro připojení databáze (Obr.67: Konfigurace – New Mailbox Database). Tlačítkem „New" vytvoření potvrdíme a zkontrolujeme zobrazenou informaci o vytvoření i připojení.

V EMS vytvoříme novou databázi a druhým příkazem databázi připojíme:
new-mailboxdatabase -StorageGroup "E2K7CCR\Second Storage Group" -Name "Mailbox Database" -EdbFilePath "C:\Program Files\Microsoft\Exchange Server\Mailbox\Second Storage Group\Mailbox Database.edb"

mount-database -Identity "E2K7CCR\Second Storage Group\Mailbox Database"

Vytvoření mailboxu k uživatelskému účtu
V EMC v sekci Recipient Configuration / Mailbox zvolíme akci New Mailbox (Obr.68: Konfigurace – EMC New Mailbox). Ve zobrazeném průvodci zvolíme typ User Mailbox (Obr.69: Konfigurace – Mailbox Introduction), vybereme existující uživatele (Obr.70: Konfigurace – Mailbox User Type) a databázi pro umístění mailboxu (Obr.71: Konfigurace – Mailbox Settings). Dokončíme vytvoření mailboxu.

Pro specifikaci kritérií při hromadném vytváření mailboxů je výhodnější použít EMS. Následující příkaz ukazuje vytvoření poštovních schránek pro všechny uživatele typu User z určité organizační jednotky a oddělení na serveru, resp. clusteru E2K7CCR v úložišti First Storage Group a databázi Mailbox Database.

get-user –organizationalUnit Ostrava |where-object {$_.RecipientType –eq "User" -and $_.department –eq "Poradci"} |Enable-Mailbox –Database "E2K7CCR\First Storage Group\Mailbox Database"

Nastavení limitů mailboxů
Pro každou poštovní databázi můžeme nastavovat limity mailboxů, délku držení smazaných zpráv nebo smazaných mailboxů.

Set-MailboxDatabase -Identity "E2K7CCR\First Storage Group\Mailbox Database" -IssueWarningQuota 2GB -ProhibitSendQuota 3GB -ProhibitSendReceiveQuota 4GB –QuotaNotificationSchedule "Sun.2:00-Sun.3:00","Wed.2:00-Wed.3:00"

Set-MailboxDatabase -Identity "E2K7CCR\First Storage Group\Mailbox Database" -DeletedItemRetention 7.00:00:00

Set-MailboxDatabase -Identity "E2K7CCRFirst Storage Group\Mailbox Database" -MailboxRetention 45.00:00:00

4.2 Client Access Server

Kromě přístupů klientů je CAS zodpovědný za přístup k automatickému nastavení profilu, k informacím o zaneprázdněnosti, ke zprávám Out of Office (OOF - mimo kancelář), k Offline adresáři a také k funkci Unified Messaging (UM), ale pouze pro Outlook 2007 a Outlook Web Access 2007. Jedině tyto dva typy klientů mohou využívat nové webové služby Exchange, známé jako AutoDiscovery a Availability. [3]

Instalací role CAS se vytvoří pod výchozím webovým serverem v IIS virtuální adresář AutoDiscover. Z tohoto adresáře získávají klienti Outlook 2007 potřebná nastavení. Výchozímu webovému serveru je přiřazen certifikát SSL s vlastním podpisem (Obr. 72: Konfigurace – IIS Web Site Certificate). Pokud společnost bude využívat připojení Outlook Anywhere nebo Exchange ActiveSync musí být výchozí certifikát nahrazen certifikátem vydaný důvěryhodnou autoritou nebo ponechán, zřídíme-li dva web servery pro službu AutoDiscover a pro připojení OWA, EAS a Outlook Anywhere. Rozdíl mezi uvedenými možnostmi je v typu použitého certifikátu. První případ vyžaduje přiřazení certifikátu, který pracuje s alternativními jmény web serveru, zatímco v druhém řešení pro dva nové web servery použijeme běžný certifikát důvěryhodného vydavatele.

Outlook Anywhere
Po instalaci SSL certifikátu přistoupíme k aktivaci služeb Outlook Anywhere.
V EMC v sekci serverová konfigurace CAS serveru z nabídky Akce zvolíme Enable Outlook Anywhere (Obr.73: Konfigurace – Enable Outlook Anywhere), vyplníme název serveru který je s hodný s názvem uvedeným v certifikátu, zvolíme typ autentizace a zda budeme využívat zabezpečenou komunikaci SSL.

EMS :
enable-OutlookAnywhere -Server "EXCH-HUBCAS"-ExternalHostname "owa.mycompany.cz"-DefaultAuthenticationMethod "Ntlm"-SSLOffloading $false

OWA, ActiveSync
Obě funkce jsou ve výchozím nastavení povoleny. Konfigurace je spojená s webovými servery a provádí se částečně v IIS a částečně v konzoli pro administraci exchange EMC nebo EMS. V IIS je pro každou službu vytvořen virtuální adresář a jeho nastavení se nachází v konfiguraci pro CAS server, ve vlastnostech pro danou službu (Obr.74: Konfigurace – Outlook Web Access , Obr.75: Konfigurace – Exchange ActiveSync).

Ve vlastnostech funkcí v EMC lze specifikovat i další nastavení související s autentizaci, přímým přístupem k souborům přes OWA nebo přístupem ke vzdáleným souborovým serverům.

POP3/IMAP
Oba klientské protokoly běží jako samostatné služby Windows a nejsou závislé na IIS. Ve výchozím nastavení jsou zakázány a je potřeba ve snap-inu pro správu služeb povolit jejich automatické spuštění.

Ve vlastnostech protokolů v EMC nebo příkazy EMS konfigurujeme vlastnosti spojené s připojením, porty, autentizací a formátem zpráv (Obr.76: Konfigurace – POP3). Po veškerých změnách provedených v administrační konzoli je pro aplikaci nastavení nutný restart příslušné služby.

4.3 Hub Transport

Kromě zodpovědnosti za vnitřní tok pošty v organizaci má Hub Transport server množinu transportních agentů, které nám umožňují nakonfigurovat pravidla a nastavení, jež pak lze aplikovat na zprávy procházející serverem. Hub Transport server také umožňuje nastavit postupy a pravidla, jež vyhovují specifickým nařízením firmy. [3]

Vlastní směrovací topologii Exchange Serveru 2007 není potřeba nastavovat, protože k informacím o umístění serverů v exchange organizaci je plně využíváno dat z Active Directory. Z pohledu serverové konfigurace lze na Hub Serveru nastavovat vlastnosti přijímacích konektorů a antispamových agentů, byli-li na Hub server instalováni.

Přijímací konektory určují způsob přijímáni zpráv na server přes SMTP protokol. Po instalaci Hub serveru jsou vytvořeny dva výchozí konektory (Default, Client) pro příjem pošty od jiných SMTP klientů. Vytvořením vlastního konektoru můžeme řídit příjem zpráv z určité IP adresy nebo bloku IP adres. V případě, že infrastruktura zahrnuje i Edge Transport, je pro provedení Edge Subscription vytvořen také přijímací konektor pro Edge.

Přijímací konektor pro příjem mailů z internetu V konfiguraci Hub serveru v EMC zvolíme akci New Receive Connector a ve spuště- ném průvodci vyplníme název a typ konektoru (Obr.77: Konfigurace – Receive Connector). Dále můžeme upravit IP adresu, port a doménový název pro odpověď na HELO a EHLO (Obr.78: Konfigurace – Connector Settings). Vytvoření nového konektoru dokončíme.
Používáme-li pro tok pošty z a do internetu Edge Transport Server, je přijímací i odesílací konektor, provedením Edge Subscription, vytvořen automaticky.

EMS:
new-ReceiveConnector -Name ”NewReceiveConnector”-Usage ”Internet”-Bindings ”192.168.1.3:25”-Fqdn ”mail.mycompany.cz”-Server ”EXCH-HUBCAS”

Ve společnostech, které nepřijímají poštu přes Edge server, musíme na výchozím konektoru Default povolit příjem pošty od anonymních uživatelů. Nastavení provedeme ve vlastnostech konektoru (Obr.79: Konfigurace – Default Connector).

4.4 Edge Transport

Instalace adresářové služby ADAM včetně konfigurace jednosměrné replikace dat z doménového řadiče interní sítě přes Hub Transport, službou Edge Sync až na Edge server v perimetru, je popsána v příloze Edge Transport Server.

Po nainstalování serverové role Edge Transport a vykonání Edge Subscription jsou automaticky vytvořeny konektory pro odesílání pošty do Internetu i na Hub Transport server společnosti. Z tohoto důvodu není vytváření dalších konektorů nutné.

Služba EdgeSync zajišťuje mimo replikace dat příjemců také přenos nastavení spojených s transportními pravidly a akceptovanými doménami vytvořených v konfiguraci exchange organizace. Konfigurace antispamu podléhá individuálním potřebám společnosti. Pomocí filtrovacích agentů nastavujeme filtrování spojení, filtrování na základě seznamů povolených a zakázaných odesilatelů a příjemců, filtrování podle obsahu a důvěryhodnosti (Obr.64: Edge – EMC).

4.5 Nastavení poštovního serveru pro celou společnost

Veškerá globální nastavení a funkce vztahující se na celou exchange organizaci se provádí v části navigačního panelu Organization Configuration. Konfigurace se člení podle serve-

rových rolí a zahrnuje množství specifických nastavení, která usnadňují práci především ve větších společnostech. Při vytváření funkcí z EMC je vždy spuštěn grafický průvodce, který si v několika málo krocích vyžádá potřebné informace a na závěr zobrazí comandlet pro přímé použití v EMS. Jelikož detailní popis konfiguračních kroků je velmi zdlouhavý, uvedu pouze informativní výčet možných nastavení pro každou serverovou rolí.

Mailbox

Address Lists
Výchozí seznamy adres slouží pro organizaci příjemců podle stanovených podmínek (oddělení, lokace, speciální atributy)

Managed Default Folders
Základní složky s řízeným obsahem, řízení obsahu představuje nastavení doby pro smazání nebo přesun položek, případně poslání kopie zpráv na určitého příjemce. Základní složky jsou např. Inbox, Calendar, Sent Items a Deleted Items.

Managed Custom Folders
Vlastní složky s řízeným obsahem umožňují vytvoření speciálních složek pro potřeby organizace a nastavení shodná se základními složkami s řízeným obsahem. Pro využití této funkce je nutné vlastnit licence Exchange Enterprise CAL.

Managed Folder Mailbox Policies
Vytvoření pravidel Mailbox Policy, do které začleníme složky s řízeným obsahem. Politiku aplikujeme na mailboxy při jejich vytváření nebo dodatečně ve vlastnostech mailboxů Mailbox Settings v sekci konfigurace příjemců

Offline Address Book
Offline adresář je vytvořen automaticky, generuje se jeden krát denně a je dostačující pro většinu společností. Další OAB se vytváří např. při potřebě rozlišit příjemce podle země nebo organizace. Offline adresář se využívá pro offline práci klientů Outlook.

CAS

Exchange ActiveSync Mailbox Policies
Vytvoření bezpečnostních pravidel zahrnuje nastavení složitosti hesla, vypršení relace z důvodu neaktivity, vzdálené smazání při opakovaných chybných pokusech o přihlášení, přenos souborů. Vytvořená pravidla se aplikují na mailboxy podobně jako Mailbox Policy v sekci konfigurace příjemců, část Mailbox Features.

Hub Transport

Remote Domains
Nastavení přenosu zpráv mezi exchange 2007 a vzdálenými externími SMTP doménami. Pro vzdálené domény můžeme řídit tok zpráv pomocí pravidel, nastavovat formátování, povolit nebo zákazat posílání zpráv Mimo kancelář.

Accepted Domains
Nastavení relaye pro zasílání zpráv přímo na e-mailový server v jiné doménové struktuře AD vlastní nebo externí společnosti. Zároveň se zde definují i vlastní domény, které Exchange server spravuje, tzv. Authoritative domains.

E-mail Address Policies
Pravidla pro definici e-mailových adres, které se vytvoří automaticky při zřízení objektu AD, jenž je příjemcem elektronické pošty. Jedná se o uživatele s mailboxem, externí uživatele s e-mailovou adresou, kontakty, sdílené mailboxy a distribuční seznamy.

Transport Rules
Transportní pravidla pro efektivnější řízení příchozích i odchozích zpráv. Můžeme stanovovat podmínky, za kterých se provede zvolená akce.

Send Conectors
Vytvoření konektoru pro odesílání e-mailových zpráv na smtp server v jiné doméně.

Edge Subscriptions
Slouží pro nastavení služby EdgeSync pro replikaci dat na Edge Transport.

Anti-Spam
Pokud jsme na Hub server instalovali antispamové agenty můžeme nastavovat stejná filtrovací pravidla jako nabízí serverová role Edge Transport.

4.6 Failover CCR

Cluster Continuous Replication je způsob zabezpečení vysoké dostupnosti mailbox databází. Řešení jsme použili při implementaci Exchange Serveru 2007 v modelech střední a velké společnosti. Instalací clusterovaného mailbox serveru jsme se již zabývali a poslední co považuji za nutné z pohledu správy zmínit je způsob předání služeb – Failover.

Předání služeb z jednoho uzlu na druhý se v případě havárie provede automaticky a není k němu potřeba zásah administrátora. Druhou možností je řízené, resp. ruční předání služeb. Ruční předání služeb lze provést snadno z EMC konzole nebo v několika krocích příkazy PowerShellu. Následující řádky budou popisovat předání služeb ze stávajícího aktivního nodu EXCH-CCRM1 na pasivní EXCH-CCRM2.

Failover z EMC
V navigačním panelu v části určené pro správu serverové role Mailbox zvolíme akci Manage Clustered Mailbox Server (Obr.80: Konfigurace – Manage Clustered Mailbox Server) a ve spuštěném průvodci vybereme cílový server. Do okna pro komentář zapíšeme důvod failoveru (Obr.81: Konfigurace – Move Clustered Mailbox Server). Předání služeb dokončíme.

Pro provední Failoveru z EMS slouží příkaz :

move-ClusteredMailboxServer -Identity E2K7CC -TargetMachine "EXCH-CCRM2" MoveComment "test failover" –Confirm:$false

Před spuštěním příkazu k předání služeb se doporučuje provést kontrolu zda se quorum nachází na aktivním uzlu, příp. quorum na aktivní uzel přesunout. Vhodná je také kontrola stavu kontinuální replikace databázových úložišť clusteru. Po provedení failoveru opět zkontrolujeme umístění quora a stav replikace úložišť. Zastavení a spuštění služby clusteru se provádí automaticky bezprostředně před a po vlastním předání služeb jako součást příkazu, avšak v případě neúspěšného pokusu o failover mohou být užitečné.

Kontrola umístění quora :

Get-ClusteredMailboxServerStatus -Identity E2K7CCR

Přesun quora z pasivního uzlu EXCH-CCRM2 na aktivní uzel EXCH-CCRM1 :

cluster WINCLUSTER group "cluster group"/move: "EXCH-CCRM1"

Kontrola statusu úložišt :

Get-StorageGroup -Server E2K7CCR — Get-StorageGroupCopyStatus

Zastavení služby :

Stop-ClusteredMailboxServer –Identity E2K7CCR -StopReason "test failover" -Confirm:$false

Spuštění služby :

Start-ClusteredMailboxServer –Identity E2K7CCR

5 Závěr

Cílem bakalářské práce je jednoduchým a přehledným způsobem porovnat možnosti poštovních serverů, které lze provozovat na Windows platformě a podrobněji se seznámit s problematikou poštovního systému Exchange Server 2007 společnosti Microsoft. V této souvislosti je zpracováno a popsáno několik návrhů implementace zmíněného poštovního systému a jeho následná instalace. Závěrečná část práce zachycuje základy konfigurace a správy.

Z pohledu dalšího vývoje projektu se nabízí možnost detailnějšího zpracování popisu konfigurace a správy poštovního systému včetně dostupných sad nástrojů. Oblast administrace Exchange Serveru 2007 je poměrně obsáhlá a proto jsou v rámci této práce uvedeny pouze základní prvky.

Jelikož je v současné době již k dispozici nová edice produktu MS Exchange Server 2010, může být popis rozdílů obou systémů společně s významným zaměřením na administraci námětem diplomové práce.

Lenka Kučerová

6 Reference

[1] ŘÍHA, Petr, *Slovník počítačové informatiky: výkladový slovník pro práci s informacemi* , 1. vyd. Montanex 2002, ISBN : 80-7225-083-3.

[2] NAUMANN, Friedrich, *Dějiny informatiky: od abaku k internetu* , 1. vyd. Academica 2009, ISBN : 978-80-200-1730-7.

[3] WALTHER, Henrik, *Jak vyzrát na Microsoft Exchange Server 2007: konfigurace správa, upgrade* , 1. vyd. Computer Press 2008, ISBN : 978-80-251-2003-3.

[4] *Kerio* [online], c2009 [cit.2010-01-15]
Dostupné z: <http://www.kerio.cz/>

[5] *IBM - Česká republika* [online], c2007 [cit.2010-02-02].
Dostupné z: < http://www.ibm.com/cz/cs/>

[6] *Microsoft* [online], c2010 [cit.2010-02-02].
Dostupné z: < http://www.microsoft.com/cs/cz/>